Proofpoint Security Awareness Training - Contenuti

Modificare il comportamento degli utenti per ridurre i rischi

PRINCIPALI FUNZIONALITÀ

Libreria di contenuti

Facile recupero dei contenuti in base a minacce, utenti, aree geografiche e formati

Programmi di studio di base

Percorsi di apprendimento guidati da CISO o esperti per accelerare l'implementazione e l'integrazione di nuovi utenti

Valutazione dell'utente

Comprensione dei punti di forza e di debolezza di utenti, gruppi e dipartimenti

Moduli di formazione

Un'ampia gamma di argomenti e formati dedicati a sicurezza e privacy per rispondere alle preferenze degli utenti

Personalizzazione e distribuzione dei contenuti

Personalizzazione dell'esperienza di apprendimento per i tuoi utenti e possibilità di distribuire i contenuti tramite il tuo sistema di formazione (LMS)

Materiali di sensibilizzazione alla sicurezza

I materiali pronti all'uso facilitano l'implementazione di campagne di sensibilizzazione efficaci e l'invio tempestivo di allarmi e rapporti sulle minacce

Traduzioni

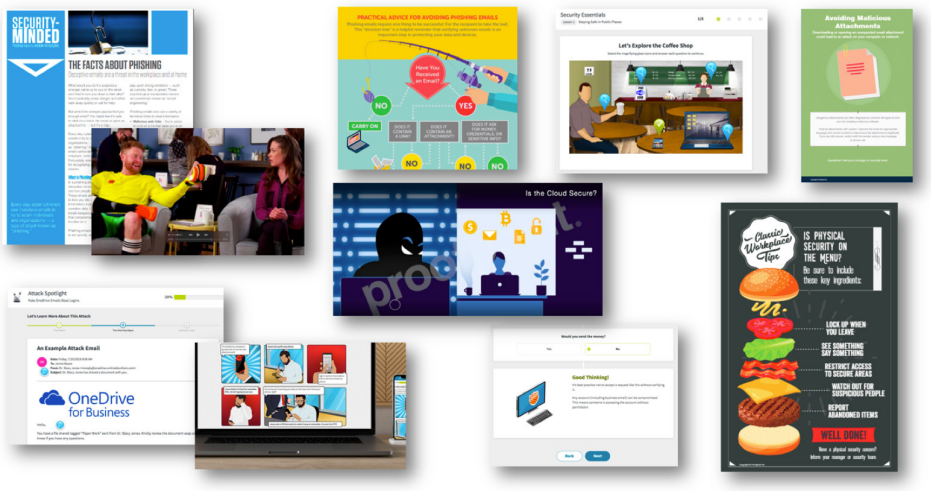
40 traduzioni per il programma di studio fondamentale e un minimo di sei per tutti i contenuti

Simulazioni

Una libreria completa di minacce simulate per aiutare a valutare la capacità degli utenti di riconoscere gli attacchi di social engineering

Proofpoint Security Awareness Training (PSAT) offre contenuti collaudati per generare un cambiamento misurabile nel comportamento degli utenti. Le nostre soluzioni ti aiutano a proporre la formazione adeguata ai dipendenti giusti al momento opportuno. Ciò assicura la reazione corretta alle minacce e ai requisiti in materia di sicurezza e privacy. Grazie alle nostre soluzioni puoi:

- Valutare e formare gli utenti
- Disporre di materiali efficaci per le campagne di sensibilizzazione alla sicurezza
- Automatizzare la reportistica
- Neutralizzare le email sospette



I contenuti Proofpoint Security Awareness Training includono un'ampia varietà di corsi e altre risorse.

Programma di studio di base, percorso di formazione e traduzioni

Accelera il cambiamento dei comportamenti attraverso programmi di base e a percorsi formativi guidati da CISO o da esperti. I programmi di studio di base forniscono agli utenti le conoscenze essenziali e li aiutano a sviluppare ulteriormente le loro competenze. In combinazione con percorsi di formazione specifici a seconda dei ruoli, le aziende possono beneficiare dei suggerimenti di esperti per accelerare l'apprendimento degli utenti e l'amministrazione della formazione.

Tutti i corsi di base sono tradotti in oltre 40 lingue e ulteriori corsi e materiali di sensibilizzazione sono disponibile in almeno 6 lingue.

Contenuti per le valutazioni: comprendere ciò di cui gli utenti hanno bisogno

Quando si tratta di pratiche di sicurezza e privacy, è importante comprendere le lacune nelle conoscenze dei dipendenti. Ti aiutiamo a offrire loro una formazione sulla sicurezza personalizzata e di identificare a livello più globale i rischi per la tua azienda.

I nostri attacchi simulati ThreatSim, che ti aiutano a valutare la vulnerabilità delle tue persone alle minacce del mondo reale, includono il phishing e attacchi USB. Con le valutazioni delle conoscenze CyberStrength puoi valutare le conoscenze dei tuoi dipendenti rispetto a una vasta gamma di argomenti fondamentali della sicurezza.

ATTACCHI SIMULATI THREATSIM - PHISHING E USB

Modelli degli attacchi simulati

Puoi valutare gli utenti in base a numerosi tipi di minaccia, che includono allegati dannosi, link incorporati, dispositivi USB con contenuti dannosi e richieste di dati personali. Puoi scegliere fra migliaia di modelli in oltre 36 lingue.

Categorie dei modelli:

- Cloud
- Commercial
- Privato
- Azienda
- Informazioni sulle minacce Proofpoint
- Stagionali
- USB
- Settoriale

Pagine di destinazione dei messaggi formativi

Puoi utilizzare dei messaggi formativi puntuali che vengono visualizzati nel momento stesso in cui un dipendente interagisce con una falsa email di phishing. Queste pagine di destinazione forniscono informazioni sulla minaccia e spiegano i pericoli associati agli attacchi reali. Inoltre, offrono dei suggerimenti per evitare attacchi futuri.

Tipi di messaggi formativi:

- Personalizzato
- Integrato
- Messaggi di errore
- Interattivo
- Video

VALUTAZIONI DELLE CONOSCENZE CYBERSTRENGTH

Valutazioni delle conoscenze personalizzate e predefinite

Puoi valutare le conoscenze degli utenti su vari argomenti al di là degli attacchi simulati. Puoi scegliere fra più di 400 domande incorporate oppure aggiungerne di tue. Puoi inoltre scegliere fra 17 valutazioni predefinite delle conoscenze in molte differenti categorie.

Valutazioni delle conoscenze predefinite:

- Valutazioni globali, 55, 33 e 22 domande
- GDPR
- Minacce interne
- Sicurezza online
- Protezione delle password
- PCI (Payment Card Industry?
- Phishing
- Dati personali
- Prevenzione delle violazioni
- Protezione delle informazioni sanitarie
- Protezione dei dati personali
- Protezione dell'email - Serie avanzata
- Protezione dell'email - Serie base
- Misure di sicurezza
- Sicurezza mobile

Moduli di formazione Proofpoint

I nostri premiati moduli di formazione flessibili sono disponibili sotto forma di giochi, video e contenuti interattivi. Si basano su principi pedagogici volti a stimolare il cambiamento dei comportamenti. I nostri moduli derivano dai servizi di threat intelligence di Proofpoint per assicurarne la rilevanza in base al mutevole panorama delle minacce.

Informazioni sui moduli

- Le lezioni sono brevi e si concentrano su un solo argomento. Il completamento dei moduli richiede in media solo 15 minuti, in tal modo l'attenzione degli utenti rimane alta durante tutta la formazione, aumentando le probabilità di apprendere e ricordare i contenuti.
- I contenuti sono personalizzabili, su misura dei tuoi utenti. Il nostro Customization Center self-service ti permette di modificare testi, schermate, immagini, domande, risposte e anche di cambiare l'ordine dei contenuti.
- Gli utenti possono essere iscritti automaticamente a un modulo di formazione particolare a seguito di una valutazione, per garantire che ricevano la formazione appropriata al momento opportuno.
- I moduli di formazione sono utilizzabili anche da dispositivi mobile e progettati per essere facilmente accessibili; inoltre rispettano lo standard U.S. Section 508 e lo standard WCAG 2.0 AA (linee guida per l'accessibilità ai contenuti Web).

Argomenti dei moduli di formazione

- Application Security (Sicurezza delle applicazioni)
- Anti-Fraud and Bribery (Lotta contro le frodi e le tangenti)
- Anti-Money Laundering (Antiriciclaggio)
- Avoiding Dangerous Attachments (Identificazione degli allegati pericolosi)
- Avoiding Dangerous Links (Identificazione dei link pericolosi)
- Business Email Compromise (Violazione dell'email aziendale)
- Compromised Devices (Dispositivi compromessi)
- Data Protection and Destruction (Protezione e distruzione dei dati)
- Email Security (Email security)
- Email Security on Mobile Devices (Email security sui dispositivi mobili)
- FERPA (Family Educational Rights and Privacy Act - Legge sulla Tutela della privacy dei dati relativi al percorso formativo degli studenti)
- GDPR - (General Data Protection Regulation - Regolamento generale sulla protezione dei dati)
- Healthcare (Sanità)
- Insider Threats (Minacce interne)
- Phishing
- Malware
- Mobile Security (Sicurezza mobile)
- Password
- PCI (Payment Card Industry - Standard del settore delle carte di pagamento)
- Physical Security (Sicurezza fisica)
- PII and Personal Data Protection (Protezione di informazioni e dati personali)
- Privileged Access Awareness (Sensibilizzazione agli accessi privilegiati)
- Ransomware
- Moduli specifici in base ai ruoli per il servizio clienti, la contabilità e la direzione
- Safe Social Networking (Utilizzo sicuro dei social network)
- Safe Web Browsing (Navigazione web sicura)
- Secure Printing (Stampare in sicurezza)
- Security Beyond the Office (Sicurezza oltre l'ufficio)
- Security Essentials (Principi fondamentali della sicurezza)
- Travel Security (Sicurezza in viaggio)
- URL Training (Formazione sugli URL)
- USB Device Safety (Sicurezza dei dispositivi USB)
- Working From Home (Telelavoro)
- Workplace Security in Action (Sicurezza sul luogo di lavoro in azione)
- Video: Workplace Security in Action (Sicurezza sul luogo di lavoro in azione)

Moduli di formazione TeachPrivacy

Collaboriamo con TeachPrivacy per ampliare la nostra gamma di contenuti e i tipi di formazione disponibili. Tutti i contenuti sono convalidati dai nostri team pedagogici e di sviluppo, in modo da garantire continuità e coerenza ai tuoi utenti.

TeachPrivacy vanta una lunga esperienza in materia di normative e di requisiti legati alla privacy. Con i suoi ricchi contenuti, puoi personalizzare la formazione in materia di privacy e conformità in base alla tua cultura aziendale e alle tue problematiche specifiche.

Argomenti di TeachPrivacy

- California Health Privacy (Obblighi di riservatezza nel settore della sanità in California)
- CCPA (California Consumer Privacy Act - Legge della California sulla riservatezza dei dati dei consumatori)
- FERPA (Family Educational Rights and Privacy Act - Legge sulla Tutela della privacy dei dati relativi al percorso formativo degli studenti)
- FTC Red Flags (Indicatori di allarme della Federal Trade Commission)
- GDPR - (General Data Protection Regulation - Regolamento generale sulla protezione dei dati)
- GLBA (Gramm-Leach-Billey Act - Legge sulle transazioni finanziarie negli Stati Uniti)
- HIPAA (Health Insurance Portability and Accountability Act - Obblighi di riservatezza e sicurezza dei dati per le organizzazioni incaricate di salvaguardare i dati sanitari protetti)
- Malware e Privacy
- PCI (Payment Card Industry - Standard del settore delle carte di pagamento)
- Privacy for Federal Government Contractors (Privacy per gli appaltatori del governo federale)
- Texas Health Privacy (Obblighi di riservatezza nel settore della sanità in Texas)
- Ransomware

Personalizzazione e distribuzione dei contenuti

Grazie al nostro Customization Center self-service, puoi adattare i contenuti ai tuoi utenti e migliorarne la pertinenza. Personalizza facilmente i corsi di formazione con testi, immagini e domande pertinenti per i tuoi utenti. Clona e modifica rapidamente i moduli, le lezioni e le pagine per apportare le modifiche necessarie, il tutto in tempo reale. È anche possibile trasformare i moduli di formazione (con domande) in moduli di sensibilizzazione con un solo clic.

Per garantire l'efficacia dei tuoi contenuti, la funzione Learning Science Evaluator ti guida con l'aiuto di commenti. Per esempio, se la lunghezza, la quantità di contenuti sullo schermo o il numero di domande di un quiz sono troppo impegnativi, verrai avvisato.

Nelle aziende che dispongono di un proprio sistema LMS che utilizza file SCORM, gli amministratori possono facilmente personalizzare ed esportare i moduli di formazione nel sistema. Possono combinare più moduli in uno solo e anche definire l'ordine in cui gli utenti devono seguirli.

Materiali di sensibilizzazione alla sicurezza

Per sostenere i tuoi progetti di formazione e di sensibilizzazione, offriamo una ricca selezione di materiali di moduli, video, poster, immagini, newsletter, articoli, infografiche, ecc. Questi materiali sono concepiti per favorire le discussioni sulla sicurezza informatica con i tuoi utenti finali. Facendo della sicurezza una priorità assoluta nella mente dei tuoi utenti, puoi ridurre il livello di rischio per la tua azienda.

- Puoi personalizzare la maggior parte dei materiali di sensibilizzazione con il logo della tua azienda. Puoi accedere ai file originali dal portale Materiali per la sensibilizzazione alla sicurezza.
- Molti dei nostri materiali di sensibilizzazione sono disponibili in 20 lingue.

Attack Spotlight e avvisi sulle minacce

Grazie alla nostra threat intelligence leader di mercato, ti aiutiamo a capire gli utenti che verranno attaccati e in che modo, assicurandoci che ricevano una formazione adeguata. Inoltre, il nostro flusso costante di threat intelligence ti offre la migliore visione delle minacce nuove ed emergenti, in modo che la formazione e la consapevolezza ricevuta dagli utenti possano consentire loro di riconoscere ed evitare nuovi pericoli.

Attack Spotlight: informa gli utenti sulle minacce attuali. Questi contenuti, rilasciati su base mensile, vengono puntualmente creati a partire dagli attacchi di phishing, dalle tecniche e dalle esche osservati sul campo dai servizi di threat intelligence di Proofpoint.

- COVID-19 (Coronavirus)
- DocuSign Phishing (Messaggi di phishing Docusign)
- Domain Fraud (Frodi dei domini)
- Dridex
- Fake Browser Updates (Falsi aggiornamenti del browser)
- Fake OneDrive Emails Steal Logins (Credenziali rubate dalle false email di OneDrive)
- Fraudulent Shipping Notifications (Avvisi di consegna fraudolenti)
- Look-Alike Websites Trick Users (Siti web fasulli per ingannare gli utenti)
- Microsoft Office 365 Credential Phishing (Phishing delle credenziali di accesso per Microsoft 365/Office 365)
- OneDrive Phishing Campaign (Campagna di phishing OneDrive)
- Phishing Campaign Delivers Dangerous Trojan (Una campagna di phishing inietta un trojan pericoloso)
- Scammers Mimic Real Banking Emails (I truffatori imitano email reali delle banche).
- Malicious Cloud Applications (Applicazioni cloud dannose)

Avvisi sulle minacce: avvisa rapidamente i tuoi utenti dell'esistenza di attacchi specifici rilevati dai servizi di threat intelligence di Proofpoint.

- COVID-19 Credential Phishing (U.S. Retailers) (Phishing delle credenziali legato al COVID-19 - Commercianti al dettaglio statunitensi)
- COVID-19 Phish Spreading Malware (U.S. Infrastructure) (Phishing legato al COVID-19 che diffonde malware - infrastrutture USA)
- WebEx Credential Phishing Lures (Esche del phishing delle credenziali legato a WebEx)
- Zoom Credential Phishing Lures (Esche di phishing delle credenziali legato a Zoom)
- Zoom Phishing Attacks Spread Malware (Attacchi di phishing legato a Zoom che diffondono malware)
- Altri avvisi ogni settimana

Video di sensibilizzazione: introduci i tuoi dipendenti all'importanza della sensibilizzazione in fatto di sicurezza con video coinvolgenti e divertenti. Ecco un esempio di oltre 50 video disponibili:

- Video di sensibilizzazione: Think Before You Click (Great Saves) (Rifletti bene prima di fare clic - Una parata eccezionale)
- Video di sensibilizzazione: Is the Cloud Secure? (Il cloud è sicuro?)
- Video di sensibilizzazione: Use Caution on Public Wi-Fi (Fai attenzione quando usi una rete Wi-Fi pubblica)
- Video The Defence Works: non particolarmente tecnico
- Video The Defence Works: Oh… My Password! (Oh, la mia password!)
- Video The Defence Works: Swiped Right Into Trouble (Scorri a destra e sei nei guai)
- 60 Seconds to Better Security (60 secondi per una migliore sicurezza): Che cos'è lo smishing?
- 60 Seconds to Better Security (60 secondi per una migliore sicurezza): Che cos'è il phishing?
- 60 Seconds to Better Security (60 secondi per una migliore sicurezza): cosa sono gli attacchi BEC?
- Ecc.

Infografiche: Utilizza questi elementi per rafforzare i principi fondamentali per un'informatica sicura:

- Attacchi che violano l'email aziendale
- Internet of Things (L'Internet delle cose)
- Phishing Decision Tree (L'albero decisionale del phishing)
- Phishing: A Scammer's Sinister Scheme (Regular and Expanded) (Phishing: il sinistro piano dei truffatori - Versione normale e versione estesa)
- Tax-Related Schemes (Truffe fiscali)
- Comprendere il ransomware
- Ecc.

Newsletter e articoli

- Newsletter e articoli sul tema della sicurezza che affrontano diversi argomenti: ritorno a scuola, collegamenti e allegati pericolosi, acquisti in vacanza, minacce interne, password, phishing, sicurezza fisica, consigli per i viaggi e molto altro.

Poster: mantengono il messaggio ben visibile e rafforzano l'apprendimento.

- Identificazione degli allegati dannosi
- Be Smart About Mobile Security (Ottimizza la protezione dei dispositivi mobili)
- La sicurezza degli URL
- Dangerous USB Devices (Dispositivi USB pericolosi)
- Is Physical Security on the Menu? (La sicurezza fisica è prevista?)
- Not All Offers Are as Sweet as They Seem (Non tutte le offerte sono così gradevoli come sembrano)
- Ecc.

Varie

- Grafiche e istruzioni per creare ulteriori contenuti
- Gioco "Cybersecurity Consequences" (Cybersecurity e conseguenze)
- Post-it "Lock Before You Walk" (Chiudi a chiave il tuo ufficio)
- Meme
- Cartoline
- Ecc.

Documentazione sul programma

Perché un programma abbia successo, tutte le persone coinvolte devono capire perché sono coinvolte e cosa ci si aspetta da loro. È per questo che i contenuti dei nostri programmi di sensibilizzazione alla sicurezza includono consigli di esperti per suggerire agli amministratori il modo più efficace di implementare il programma. Forniamo inoltre delle comunicazioni mirate per gli utenti e le parti interessate principali. I nostri materiali sono organizzati in quattro categorie:

- Le migliori pratiche
- Le chiavi del successo
- Campagne

Queste informazioni aiutano gli amministratori del tuo programma di formazione a generare un rapporto di fiducia con gli utenti e a creare una cultura di sensibilizzazione alla sicurezza.

Le migliori pratiche: la nostra documentazione sulle migliori pratiche aiuta gli amministratori del programma a stimolare un cambiamento efficace dei comportamenti. Non importa se il tuo programma è nuovo o se è in vigore già da tempo: Questi contenuti ti forniscono informazioni sulle tempistiche, le migliori pratiche e i piani suggeriti per l'implementazione di un programma.

Campagne: le campagne semplificano l'amministrazione e ti aiutano a creare delle esperienze utente ottimali. Includono tutti i contenuti e le risorse per le comunicazioni interne che ti servono per implementare un'iniziativa di sicurezza multicanale all'interno della tua azienda.

Le chiavi del successo: questi podcast, webinar, ricerche e altri contenuti sono creati per aiutare gli amministratori a spiegare il valore di un programma Security Awareness Training ai principali destinatari, a stimolare la partecipazione a corsi di formazione supplementari, a guidare le discussioni sul modello delle conseguenze e molto altro ancora. Sono disponibili presentazioni con testo scritto e pre-registrate che coprono svariati argomenti, fra cui il phishing, il furto di identità e il social engineering. Gli amministratori possono usarle per i corsi svolti di persona o per sessioni online.

APPROFONDISCI

Prova le versioni demo dei nostri moduli formativi e consulta i nostri materiali di sensibilizzazione alla sicurezza sulla pagina **https://www.proofpoint.com/it/resources/try-security-awareness-training**.