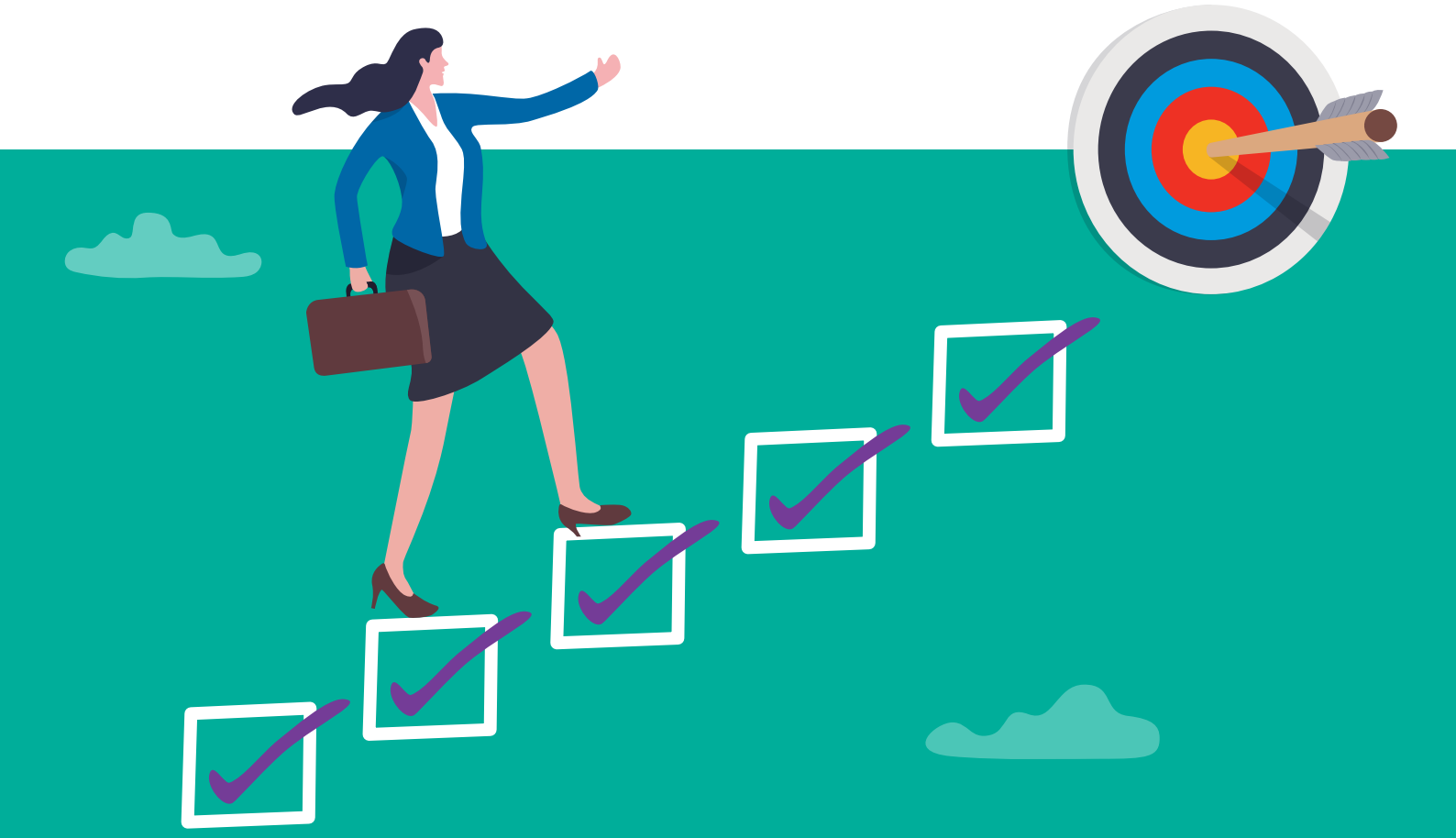
proofpoint.

EBOOK

EDIZIONE 2023

Promozione di un reale cambiamento del comportamento

Guida completa alla creazione di un programma di sensibilizzazione alla sicurezza che funzioni realmente



Collocare le persone al centro delle attività di sicurezza informatica

La minaccia informatica più potente che esista oggi non è un malware con vulnerabilità zero-day o l'ultimo kit di exploit. Sono i tuoi utenti.

Questo succede perché gli attacchi di oggi prendono di mira le persone, non l'infrastruttura IT. A prescindere dalla forma che assumono, per attivare gli attacchi informatici serve in genere una vittima umana. Gli attacchi inducono le persone ad aprire allegati pericolosi, a fare clic su URL dannosi, a fornire credenziali sul proprio account o anche a compiere azioni dirette, come l'invio di denaro o di dati sensibili.

Perché la formazione degli utenti è essenziale

In base al report 2022 sulle violazioni dei dati, l'82% di tutte le violazioni implica un intervento umano. Come si legge nel report, il malware e le credenziali rubate entrano in gioco in un secondo tempo, dopo che un attacco di social engineering ha aperto le porte ai criminali informatici, il che sottolinea l'importanza di un solido programma di sensibilizzazione alla sicurezza[1].

La formazione per la sensibilizzazione degli utenti è uno dei passi più importanti che tu possa compiere per proteggere la tua azienda. Insegnando ai tuoi utenti a riconoscere, respingere e segnalare i tentativi di phishing, puoi creare una solida ultima linea di difesa contro le principali minacce informatiche di oggi.

Cosa ti insegna questa guida

Avviare un nuovo programma di formazione può incutere un certo timore. Conservarne uno che mantenga i tuoi utenti impegnati, che modifichi il loro comportamento e riduca l'esposizione della tua azienda alle minacce può rappresentare un'impresa ancora più ardua.

Ma puoi contare su di noi.

Questa guida illustra come creare e sostenere un programma di sicurezza informatica efficiente ed efficace, a prescindere da quanto sia avanzato il programma esistente, da chi ne sia il fornitore o da quali siano gli ostacoli che devi affrontare. Fornisce fatti essenziali, strategie efficaci, risorse valide e suggerimenti pratici ai leader della sicurezza in ogni fase del viaggio verso la sensibilizzazione alla sicurezza.

Ecco alcune delle domande alle quali ti aiuteremo a rispondere:

- Come faccio ad assicurarmi che venga ben accolto? Con chi devo collaborare internamente?
- Cosa devo fare? Con che frequenza?
- Come faccio a coinvolgere il mio personale?
- Come faccio a misurare e condividere il successo?

82%

delle violazioni implica un intervento umano[1].

1 Verizon, "2022 Data Breach Investigations Report (Report 2021 sulle violazioni dei dati)", giugno 2022.

Un modello incentrato sulle persone per la misurazione e la mitigazione del rischio utente

Così come le persone sono uniche, altrettanto è il loro valore per i criminali informatici e i rischi che rappresentano per l'azienda. In Proofpoint, abbiamo creato il modello Very Attacked People (VAP)™ per misurare e contenere tre diversi aspetti del rischio utente.

La formazione per la sensibilizzazione alla sicurezza è più direttamente correlata alla vulnerabilità dell'utente. Ma il tuo programma deve anche tenere conto dei profili di attacco e del privilegio degli utenti. Queste informazioni ti consentono di adottare un approccio incentrato sulle persone alla sensibilizzazione dell'utente che comprende formazione di follow-up personalizzata, proattiva e mirata.

V

Vulnerabilità

Consente di valutare con quanta probabilità i tuoi utenti finiranno per cadere vittima di un attacco in ragione della loro predisposizione alle tattiche dei criminali informatici o ad abitudini digitali rischiose. Può essere misurata mediante valutazioni della conoscenza, con quiz per la formazione per la sensibilizzazione alla sicurezza e con simulazioni di attacchi di phishing.

A

Profilo dell'attacco

Il profilo quantifica il volume e la sofisticatezza degli attacchi e dei criminali informatici che prendono di mira gli utenti. Può anche tenere conto di utenti correlati o simili, interni ed esterni all'azienda.

P

Privilegi

Questo criterio permette di stabilire il valore e la sensibilità di dati, sistemi e risorse a cui l'utente ha accesso. Può anche essere visto come un metodo per misurare la portata del danno che un attacco riuscito può causare contro l'utente.

Sommario

SEZIONE 1

Cosa bisogna sapere prima di cominciare

Ce l'hai fatta. Il processo di approvvigionamento si è finalmente concluso. Il tuo nuovo fornitore di sensibilizzazione alla sicurezza invia un link al tuo software e il mondo ti appartiene. Sei pronto per iniziare a lanciare attacchi di phishing simulato, a raccogliere dati, ad assegnare formazione e a utilizzare tutte le caratteristiche e i contenuti straordinari che hai visto nelle demo del prodotto.

Invii l'annuncio relativo al programma di sensibilizzazione alla sicurezza. Immediatamente la tua casella di posta in entrata è inondata di risposte:

- Chi ha approvato questo esercizio?
- Ne parlerò con il mio vicepresidente.
- Devo davvero farlo?

Sono alcuni dei primi ostacoli che i nostri clienti si trovano generalmente a dover affrontare. Ma forniscono anche indicazioni preziose sulle misure che puoi adottare per garantire un programma di sensibilizzazione alla sicurezza riuscito: ottenere l'accoglienza favorevole degli utenti.

Un tema comune che i clienti ci riferiscono è che alcuni utenti non desiderano venire coinvolti nella formazione per la sensibilizzazione alla sicurezza.

Conquistare gli utenti

Un tema comune che i clienti ci riferiscono è che alcuni utenti non desiderano venire coinvolti nella formazione per la sensibilizzazione alla sicurezza. Forse gli attacchi simulati fanno sentire gli utenti vulnerabili. Altri invece potrebbero vedere la formazione come l'ennesima esercitazione aziendale nonché distrazione dal loro "vero" lavoro.

Ecco alcuni metodi per superare questo ostacolo comune:

Comunicare pensando ai vantaggi per gli utenti. Quando prepari le comunicazioni destinate agli utenti, tieni sempre presente la domanda che gli utenti si staranno ponendo: "E io che ci guadagno?". Cita esempi reali come il furto d'identità, l'appropriazione di carte di credito, le violazioni dell'account e altri ancora. Illustra in che modo la formazione può aiutare gli utenti nella loro vita personale. Ciò permetterà loro di relazionarsi meglio al programma e di migliorare la partecipazione.

Trova il giusto equilibrio tra valutazioni e formazione. Le valutazioni del phishing simulato sono componenti comuni dei programmi. A volte tuttavia se ne abusa. Molti clienti ci hanno parlato della loro esigenza di equilibrare valutazioni, formazione e attività di sensibilizzazione. Come ci ha detto un cliente: "Quando invio soltanto le simulazioni di phishing, gli utenti pensano che stiamo tentando di ingannarli." È bene trovare un equilibrio tra entrambi gli elementi in un programma, oltre alla sensibilizzazione e ad altre attività come i concorsi.

Mostrati amichevole agli eventi aziendali. La formazione e le valutazioni tramite computer possono apparire impersonali. Avere uno stand a uno dei grandi eventi aziendali o proporre sessioni virtuali come i webinar può offrire agli utenti un contatto più personale. Inizia con un incontro di avvio per i collaboratori, pianifica eventi didattici e fornisci risorse utili. Valuta di distribuire prodotti promozionale o anche solo un caffè. Queste iniziative consentono di umanizzare il programma abbinandolo a un volto e a un nome cortesi.

Superamento delle resistenze

In base alle conversazioni con i clienti, è emerso che gli utenti non coinvolti rientrano in genere in due categorie:

- **Recidivi:**utenti che non riescono mai a superare le simulazioni di attacchi di phishing e altre valutazioni
- **Non partecipanti:** utenti che si rifiutano di partecipare alla formazione

È possibile che tu abbia provato di tutto per mediare con questi utenti: email, conversazioni di persona, incontri con i responsabili o anche rimozione dell'accesso alla rete. Se malgrado tutto non sei riuscito a cambiare il loro comportamento, non hai ancora giocato l'ultima carta.

Un cliente aveva adottato la strategia per cui il CISO e gli altri responsabili programmavano incontri di 15 minuti sui calendari di questi utenti per affrontare i seguenti argomenti:

- Importanza del comportamento degli utenti e della sensibilizzazione alla sicurezza.
- Come il reparto tenta di proteggere l'azienda e gli utenti in situazioni personali.
- I motivi per cui i collaboratori devono impegnarsi a diventare più vigili o a partecipare alla formazione per contribuire

Questo genere di interazione lascia sempre una buona impressione. Comunica l'importanza del comportamento virtuoso e di una partecipazione più coinvolta in modo più personale e tangibile.

La segnalazione del phishing da parte degli utenti: una lama a doppio taglio

In occasione d una delle nostre conferenze annuali, al termine di una presentazione un cliente ha dichiarato quanto segue.

“I miei utenti non segnalano nessuna email di phishing nella nostra casella di posta per gli abusi”. “Si tratta solo di spam o di messaggi legittimi. Il nostro team non riesce a tenere il passo. In che modo dobbiamo occuparcene?”

Le caselle di posta per gli abusi sono un ottimo sistema per ridurre il rischio. Ma è risaputo che la loro gestione richiede molto tempo. Abbiamo individuato due soluzioni per questo comune ostacolo:

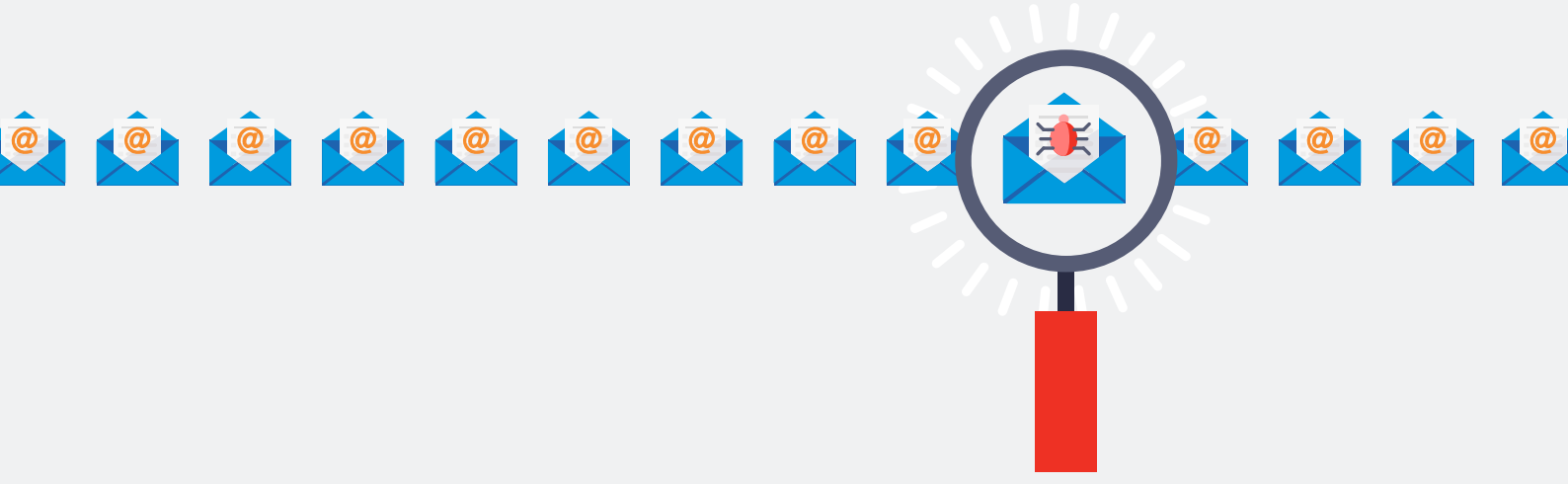
- Fare in modo che gli utenti siano più efficaci a individuare le email di phishing.
- Automatizzare il processo di analisi e risposta alle email di phishing segnalate.

Il miglioramento delle segnalazioni sarà il risultato naturale di un programma di sensibilizzazione alla sicurezza efficace. Molti clienti vedono il miglioramento nella segnalazione (più messaggi dannosi effettivi e meno falsi positivi) solo da 6 a 12 mesi dopo la distribuzione di un programma uniforme che addestra gli utenti a identificare le email di phishing.

Il miglioramento delle segnalazioni sarà il risultato naturale di un programma di sensibilizzazione alla sicurezza efficace.

Automatizzare l’analisi e la risposta alle email può alleviare i carichi di lavoro grazie all’analisi e all’arricchimento automatici tramite il sandboxing e la threat intelligence. Il team IT è meno sollecitato grazie alla rimozione automatica dei contenuti dannosi dalle caselle di posta in entrata degli utenti e dall’esclusione dei falsi positivi.

Un altro vantaggio della risposta automatica è che gli utenti possono ricevere un feedback personalizzato che li avvisa se il messaggio che hanno segnalato era realmente dannoso. Questo passaggio consente di educare gli utenti e migliora la sicurezza, rafforzando il comportamento positivo con un semplice ringraziamento per avere segnalato l’email dannosa.



SEZIONE 2

Tempistica del programma

La tempistica non è solo un particolare isolato della formazione per la sensibilizzazione alla sicurezza ma è piuttosto la somma di tutte le attività svolte. Sono la formazione giusta, le persone giuste e molti altri componenti tattici, organizzativi e strategici che confluiscono nell'esito complessivo del "momento giusto".

Ogni azienda è unica e non esistono due programmi di formazione identici.
Il tuo programma deve tuttavia includere i seguenti elementi:

- Definizione delle esigenze di formazione
- Individuazione degli utenti con esigenze formative specifiche
- Definizione delle attività
- Creazione e gestione dei programmi
- Comunicazione e verifica dei primi passaggi
- Definizione di frequenza e tempistica delle attività del programma

Ordine consigliato delle attività: lista di controllo

Un principio cardine della sicurezza informatica incentrata sulle persone è che ogni utente è diverso.

Il successo tuo programma dipende dall'attenzione con cui lo progetti e da una buona pianificazione. Di seguito sono riportati i passaggi che sono stati utili per i nostri clienti.

1. **Definire le esigenze di formazione.**

   La sicurezza informatica incentrata sulle persone inizia con la misurazione del rischio utente. Le valutazioni degli utenti forniscono indicazioni utili sui punti in cui gli utenti potrebbero essere più vulnerabili e su quali sono i compiti di formazione di cui hanno bisogno per migliorare la propria comprensione di argomenti critici quali phishing, protezione dei dati, sicurezza dei dispositivi mobili e molto altro ancora.

   Il rischio non esiste nel vuoto. Una parte essenziale dell'individuazione delle esigenze formative è comprendere l'attuale panorama delle minacce. È qui che la threat intelligence gioca un ruolo fondamentale. Una threat intelligence reale e aggiornata aiuta a comprendere le minacce correnti ed emergenti che gli utenti potrebbero trovarsi davanti.

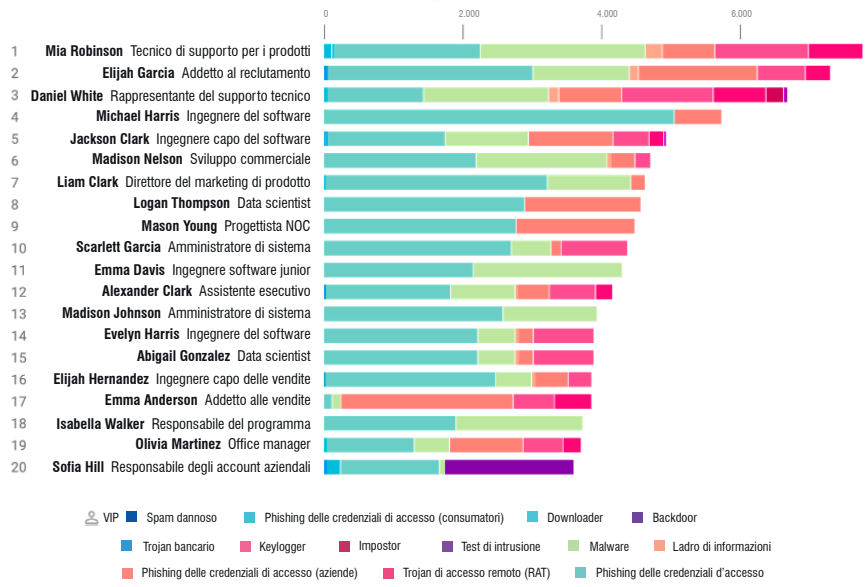
2. **Identificare utenti e gruppi a cui possono servire programmi diversi o formazione personalizzata in base alle loro esigenze.**

   Un principio cardine della sicurezza informatica incentrata sulle persone è che ogni utente è diverso. Una difesa uguale per tutti non funziona nell'ambiente odierno, e questo vale anche per i programmi di sensibilizzazione alla sicurezza.

   Questi gruppi possono richiedere formazione personalizzata o specializzata:

   - VAP**:** utenti che rappresentano un rischio elevato perché sono particolarmente vulnerabili alle tattiche dei criminali informatici, sono presi di mira più pesantemente dagli attacchi o hanno accesso a dati, sistemi o risorse di valore.

Un report VAP di Proofpoint Targeted Attack Protection



- VIP: dirigenti di massimo livello, membri del consiglio d'amministrazione e personale di alto profilo che potrebbero richiedere formazione e indicazioni specifiche a causa della loro importanza all'interno dell'azienda. Molti VIP possono essere anche VAP.
- Ruoli e reparti designati: gli utenti nei reparti risorse umane, finanziario, legale, conformità, sviluppo o con altri ruoli possono richiedere formazione obbligatoria o altra formazione specifica. Valuta di istituire valutazioni della conoscenza e simulazioni diversificate per questi gruppi man mano che il programma di formazione matura.

3. **Definizione delle attività essenziali da includere nel programma.**

   Un programma di formazione riuscito prevede il giusto mix di valutazioni, formazione, materiale didattico, comunicazioni e attività virtuali o in presenza. Di seguito sono riportati degli elementi che dovresti includere nel tuo:

   - Valutazioni degli utenti per misurare conoscenza e vulnerabilità. Possono prevedere valutazioni delle conoscenze e phishing simulato, attacchi USB e di SMiShing (phishing tramite SMS/testo).
   - Formazione tramite computer creata sulle esigenze degli utenti e sull'attuale panorama delle minacce
   - Attività di sensibilizzazione (poster, webinar, newsletter, video) per introdurre concetti e ribadire messaggi chiave.
   - Attività in presenza e virtuali come colazioni formative lunch-and-learn o webinar. Libera la creatività. Alcuni dei nostri clienti, ad esempio, hanno creato escape room di sicurezza informatica che hanno riscontrato un enorme successo.

4. **Verifica e comunica i primi passaggi.**

   Per molte aziende, un programma di formazione per gli utenti completo può rappresentare un notevole cambiamento. Comincia con un piccolo gruppo di utenti per limare le eventuali spigolature. Comunica i primi passaggi presto e spesso a tutti. Mantieni al minimo le sorprese.

   Due mesi prima del lancio

   Invia un test di simulazione di phishing a un piccolo gruppo al corrente della cosa per mettere in luce eventuali problemi tecnici nascosti. Invia quindi un test di phishing di base moderatamente difficile a tutti i collaboratori.

   Per il momento, indirizza gli utenti che abboccano alla tua esca di phishing a una pagina 404 "site not found". (Più avanti potrai indirizzare gli utenti che fanno clic a una pagina di destinazione sulla formazione.)

   Un mese prima del lancio

   Annuncia il programma agli utenti Se implementi un componente aggiuntivo di segnalazione delle email, illustrane la finalità e spiega come utilizzarlo. E se hai accesso a contenuti quali poster, immagini o altro materiale per la sensibilizzazione alla sicurezza, inviali in giro per l'ufficio o su una wiki relativa al programma.

5. **Definizione di frequenza e tempistica delle attività del programma.**

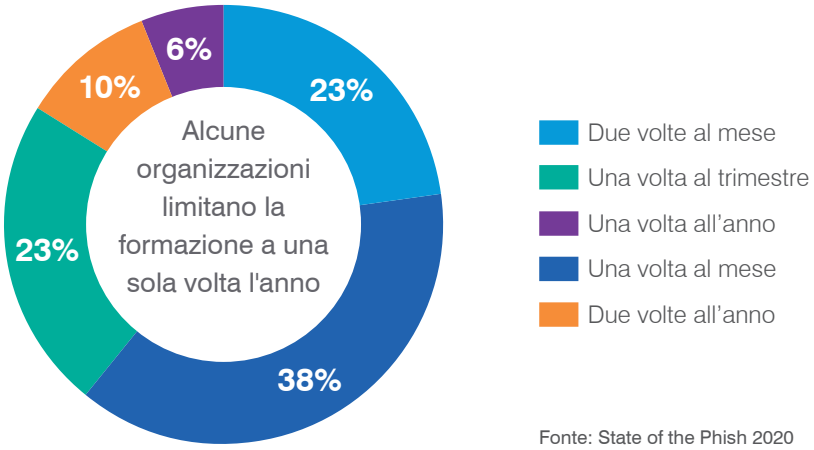
   Ancora una volta, la tempistica è tutto. Ti consigliamo di adottare la seguente cadenza per le attività di sensibilizzazione alla sicurezza:

   - Invia un test di phishing ogni 4-6 settimane. Nel farlo, pensa a variare i tipi di temi e di esche utilizzati.
   - Utilizza l'iscrizione automatica ai test di phishing almeno una volta a trimestre. Utilizza un modulo di formazione di follow-up mirato in base al tipo di attacco lanciato.
   - Esamina i report VAP ogni mese o ogni due mesi. In base a ciò che evidenzia, decidi chi deve ricevere la formazione mirata e quali contenuti didattici utilizzare.
   - Assegna formazione a livello aziendale almeno una volta a trimestre.
   - Ripeti le valutazioni sulla conoscenza a maglie più larghe e i test di phishing almeno una volta l'anno per confrontare le valutazioni di base.
   - Per rafforzare il consolidamento dell'apprendimento, programma almeno due attività di sensibilizzazione alla sicurezza all'anno tra cui webinar, concorsi o, se possibile, attività in presenza.

Crea un quadro annuale per pianificare tutte le componenti e la tempistica delle attività di formazione. Mantieniti flessibile, modificando la programmazione in base alle variazioni del più ampio panorama delle minacce.

Il nostro report State of the Phish 2020 ha rilevato che la formazione di sensibilizzazione alla sicurezza è progredita; da una cadenza annuale e trimestrale delle attività è diventata un evento mensile o anche quindicinale. Consigliamo una formazione mensile o più ravvicinata, incluse formazioni mirate, campagne di sensibilizzazione e valutazioni della conoscenza.

Frequenza della formazione per la sensibilizzazione alla sicurezza



Fonte: State of the Phish 2020

Quando cambiare

Il panorama delle minacce è in costante evoluzione. Ecco perché il nostro programma di sensibilizzazione alla sicurezza richiede un approccio continuo. A partire dalla base di valutazione iniziale, le valutazioni future possono permetterti di rilevare la competenza dell'utente e di pianificare modalità di riduzione del rischio.

Qui vengono illustrate le situazioni che richiedono la modifica della frequenza o dell'ordine delle attività di formazione:

- **Quando aumenta la prevalenza delle minacce specifiche per utente o i criminali informatici utilizzano un marchio o un'esca specifici.** Modifica il contenuto della valutazione, come ad esempio i modelli per campagne di phishing simulato, o utilizza i contenuti didattici promossi dalle minacce per gestire meglio il rischio.
- **Se la tua azienda subisce un incidente, come una violazione dei dati.** Valuta di aggiornare le attività pianificate e la frequenza delle comunicazioni, le valutazioni e la formazione relativi a tale evento.
- **Se nuove normative o disposizioni richiedono una formazione più estesa.** Procedi a una valutazione della conoscenza personalizzata per vedere in che misura gli utenti hanno assimilato i contenuti della formazione.
- **Quando la tua azienda pubblica o aggiorna una policy o nutre dei dubbi circa la conoscenza dell'utente di una policy esistente.** Una valutazione personalizzata della conoscenza può aiutarti a individuare le lacune degli utenti e indirizzare le attività di formazione.
- **Se un programma di sensibilizzazione alla sicurezza è stato interrotto per più di sei mesi.** In tal caso, potrebbe essere sensato rilanciare il programma per garantire che gli utenti ne comprendano il contesto e l'importanza.

Non consigliamo di accelerare eccessivamente la frequenza della formazione, neanche con i recidivi che hanno difficoltà con le valutazioni. Valutazioni di phishing mensili e iscrizione selettiva degli utenti che non superano uno specifico corso di formazione rappresentano un approccio ragionevole e mirato. Ma assegnare agli utenti quattro sessioni di formazione potrebbe sembrare una punizione e indurli a essere infastiditi dal programma.

Soprattutto, non cercare di fare tutto contemporaneamente. Inizia subito con l'analisi adeguata, sostenuta dalla threat intelligence e dalle valutazioni. Da lì, muoviti su tutta l'azienda per creare un piano realistico che tutti possano sottoscrivere.

Il panorama delle minacce è in costante evoluzione. Ecco perché il nostro programma di sensibilizzazione alla sicurezza richiede un approccio continuo.

SEZIONE 3

L'importanza del coinvolgimento

Potrebbe sembrare ovvio che la formazione per la sensibilizzazione alla sicurezza sia intrinsecamente un'attività incentrata sulle persone. Si propone di mettere le persone in condizione di riconoscere gli attacchi a loro destinati e di modificare il comportamento degli utenti.

Ecco perché mantenere gli utenti impegnati è essenziale per un programma efficace. Ma anche i programmi con le migliori intenzioni possono diventare noiosi se non offrono esperienze significative e pertinenti.

Mantenere gli utenti impegnati è essenziale per un programma efficace.

I programmi più riusciti:

- Usano il branding per chiarire agli utenti quanto siano importanti.
- Adottano principi didattici scientificamente testati per modificare il comportamento.
- Rafforzano la formazione con un mix diversificato di contenuti e media.
- Reclutano sostenitori su tutta l'azienda per il supporto e i miglioramenti.
- Guidano gli utenti con il giusto equilibrio tra incentivi e conseguenze.

Pensa a questi cinque principi come ai pilastri del quadro di un programma efficace che gli utenti giudicano importante. I clienti di un vasto spettro di settori hanno utilizzato questi concetti per creare programmi di formazione per la sensibilizzazione alla sicurezza volti a ridurre il rischio, tagliare i costi e supportare la conformità alla privacy dei dati.

Assegna un brand al tuo programma

Il nome giusto può consentire agli utenti di capire cosa sia il programma di formazione per la sensibilizzazione alla sicurezza e perché deve essere importante per loro.

Ad esempio, alla tua azienda può servire che gli utenti trattino i dati dei clienti dell'Unione Europea con la massima cautela per ottemperare al GDPR. Un titolo semplice e facile da dimenticare come "Formazione GDPR" potrebbe non essere adatto a promuovere negli utenti il grado di coinvolgimento necessario per stimolare modifiche del comportamento.

Un tema più efficace potrebbe essere "Diventa un difensore della privacy dei dati". Il titolo sottolinea chiaramente la finalità del programma (privacy dei dati) e il ruolo dell'utente (un partecipante attivo alle attività a favore della privacy).

La cultura dell'azienda potrebbe richiedere un approccio più diretto, con temi più pratici. Anche in quel caso, tuttavia, è comunque preferibile assegnare nomi legati ad argomenti specifici, come phishing, social engineering, email o telelavoro.

Utilizzo di principi pedagogici comprovati

Il tuo programma deve affidarsi alla pluridecennale scienza dell'apprendimento per la didattica, la memorizzazione e il cambiamento del comportamento più efficaci. Un programma ben concepito propone conoscenze concettuali e procedurali per offrire agli utenti il quadro generale e lezioni specifiche. Di seguito vengono illustrate alcune tecniche collaudate:

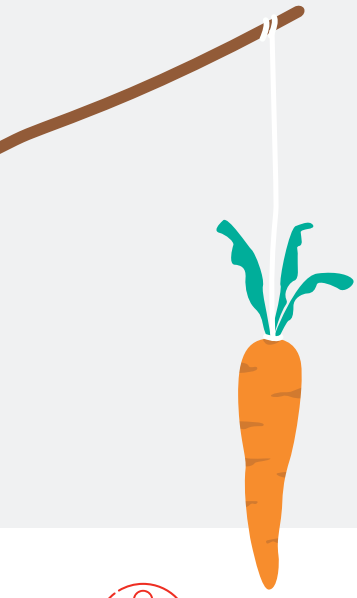
- **Trasmettere le conoscenze poco alla volta.** Limitare la formazione a qualche minuto (invece di più ore) e focalizzarsi su un unico argomento il più spesso possibile.
- **Ritornare sulle lezioni.** Fornire un feedback e mantenere persistenti formazione e sensibilizzazione.
- **Contestualizzare la formazione.** Assegnare formazione pertinente ai ruoli e alle minacce.
- **Fornire un feedback immediato.** Comunicare in tempo reale i risultati della formazione o degli esercizi di phishing.
- **Lasciare che siano gli utenti a stabilire il ritmo dell'apprendimento.** Ognuno è diverso e impara con i propri tempi.
- **Raccontare una storia.** Fornire esempi reali.
- **Variare i messaggi.** Assicurarsi di avere, per ogni argomento, più contenuti che variano per formulazione e fraseologia.
- **Coinvolgere gli studenti.** Contenuti ed esercizi interattivi agevolano la memorizzazione.
- **Fare riflettere.** Gli esercizi devono mettere alla prova la capacità degli studenti di mettere in pratica le proprie conoscenze.
- **Misurare i risultati.** Valutare direttamente gli studenti e rilevare continuamente i progressi.

Utilizzo di contenuti e media diversificati per mantenere interessante la formazione

In base alla “regola del sette”, i pubblicitari devono presentare il loro messaggio a un cliente potenziale almeno sette volte prima che venga assimilato. Il processo di apprendimento è simile.

A prescindere dalla soluzione di formazione per la sensibilizzazione alla sicurezza utilizzata, erogare le lezioni mediante più canali e attività. Ecco alcuni esempi di attività e canali che puoi utilizzare.

ATTIVITÀ	CANALI
Simulazioni di attacco (phishing, USB, SMS ecc.)	Strumenti di formazione per la sensibilizzazione alla sicurezza
Valutazioni della conoscenza	Strumenti di formazione per la sensibilizzazione alla sicurezza o strumento per sondaggi
Individuazione e monitoraggio VAP	Threat intelligence/gateway email
Formazione informatica	Moduli di formazione per la sensibilizzazione alla sicurezza tramite una piattaforma online o altro learning management system (LMS).
Campagne di sensibilizzazione	Poster, video, podcast, webinar, oratori ospiti, infografica
Esercizi di sensibilizzazione e di formazione in presenza o virtuali	Colazioni formative lunch-and-learn, webinar, stand agli eventi aziendali, interventi orali agli eventi aziendali, formazione in presenza, escape room
Concorsi/gamification	Riconoscere un cambiamento positivo del comportamento tramite un canale aziendale esistente come una newsletter o una wiki
Informazioni sulla sensibilizzazione alla sicurezza	Wiki e intranet aziendale, calendario aziendale condiviso
Aggiornamenti della sensibilizzazione alla sicurezza	Newsletter aziendale, applicazioni di comunicazione (come Microsoft Teams e Slack) o integrazione nelle comunicazioni di un altro dipartimento interno
Feedback dell’utente sul programma di formazione per la sensibilizzazione alla sicurezza	Strumento per sondaggi o casella postale condivisa
Documentazione di phishing utenti	Soluzione con componente aggiuntivo di documentazione email interno al client o indirizzo della casella di posta per gli abusi



Quando gli utenti hanno una scarsa opinione della formazione per la sensibilizzazione alla sicurezza della propria azienda, potrebbero restare indifferenti o persino opporre resistenza.

Coinvolgimento di altri dipartimenti interni e figure in ruoli chiave

I responsabili del marketing, i team della sicurezza IT e delle risorse umane oltre a altri dirigenti possono rivestire un ruolo importante nel tuo programma. Sfrutta le loro competenze per supportare e migliorare il tuo approccio, i contenuti e l'erogazione.

Ecco alcuni modi in cui gli altri reparti possono risultare utili:

- **Il team della sicurezza IT** può consigliare contenuti adattati alle policy aziendali (ad esempio le policy relative alle password). Può anche mettere in luce gli utenti che richiedono una formazione più approfondita perché vengono presi di mira più pesantemente negli attacchi informatici o per gestire dati sensibili.
- **Il marketing** può contribuire alla progettazione del materiale di sensibilizzazione alla sicurezza e di altri contenuti affinché siano in linea con gli elementi del marchio della tua azienda.
- **I team delle risorse umane** possono fornire consigli sulle dinamiche organizzative e fornire informazioni utili sulla collaborazione con dirigenti e responsabili delle linee di produzione.
- **Il CISO** (o altri C-level o membri della dirigenza) può fornire il proprio supporto e sottolineare l'importanza del programma.

Carota e bastone: indurre gli utenti ad adottare un comportamento migliore

Quando gli utenti hanno una scarsa opinione della formazione per la sensibilizzazione alla sicurezza della propria azienda, potrebbero restare indifferenti o persino opporre resistenza. Fino ad ora, abbiamo illustrato i passaggi che possono consentire di impostare un programma che venga ben accolto e che dimostri un valore reale. Quando si tratta di approcci in stile "carota e bastone" alla formazione, la maggior parte dei nostri clienti preferisce la carota.

Di quando in quando, tuttavia, la resistenza degli utenti può richiedere l'uso del bastone. In questi rari casi, un modello consequenziale può consentire di garantire la conformità alle policy di formazione. Sebbene si tratti di un'ultima possibilità, presentiamo alcuni dei modelli consequenziali utilizzati dai nostri clienti:

- Applicazione del principio delle "tre possibilità" in cui gli utenti che fanno clic su tre email di simulazioni di attacchi di phishing dovranno sostenere come conseguenza un colloquio con il loro responsabile, si vedranno privare temporaneamente del loro accesso di rete o dei loro privilegi di accesso
- Conseguenze come: rapporti delle risorse umane, riduzioni di stipendio, bonus o indennità e, in rari casi, licenziamento

Una best practice consiste nel concentrarsi su incentivi sul modello carota e utilizzare i modelli consequenziali solo come ultima opzione. I nostri clienti ritengono che affidarsi eccessivamente a questi modelli renda gli utenti meno disponibili a farsi coinvolgere nel programma. Ma se si opera in un settore rigidamente regolato o particolarmente sensibile, il bastone potrebbe rivelarsi necessario.

SEZIONE 4

Il ruolo essenziale dei dati

Dopo avere ottenuto l'approvazione per eseguire il tuo programma di sensibilizzazione alla sicurezza, sarai probabilmente desideroso di iniziare subito con gli attacchi di phishing simulato e con la formazione utente avanzata.

Tuttavia, è importante iniziare con un piano strategico. Per massimizzare i vantaggi (minore rischio per l'utente) e ridurre i costi (tempo degli utenti), le prime cose da fare dovrebbero essere fornire competenze di base, comprendere le vulnerabilità degli utenti e concentrare la formazione dove è maggiormente necessaria.

Impostazione delle basi

Il tuo primo istinto come esperto di sicurezza potrebbe essere quello di simulare attacchi di phishing avanzati o addestrare gli utenti a identificare le principali minacce che la tua azienda deve affrontare. È certamente un impulso condivisibile, ma non avrà l'impatto che speri se i tuoi utenti non hanno assimilato le basi.

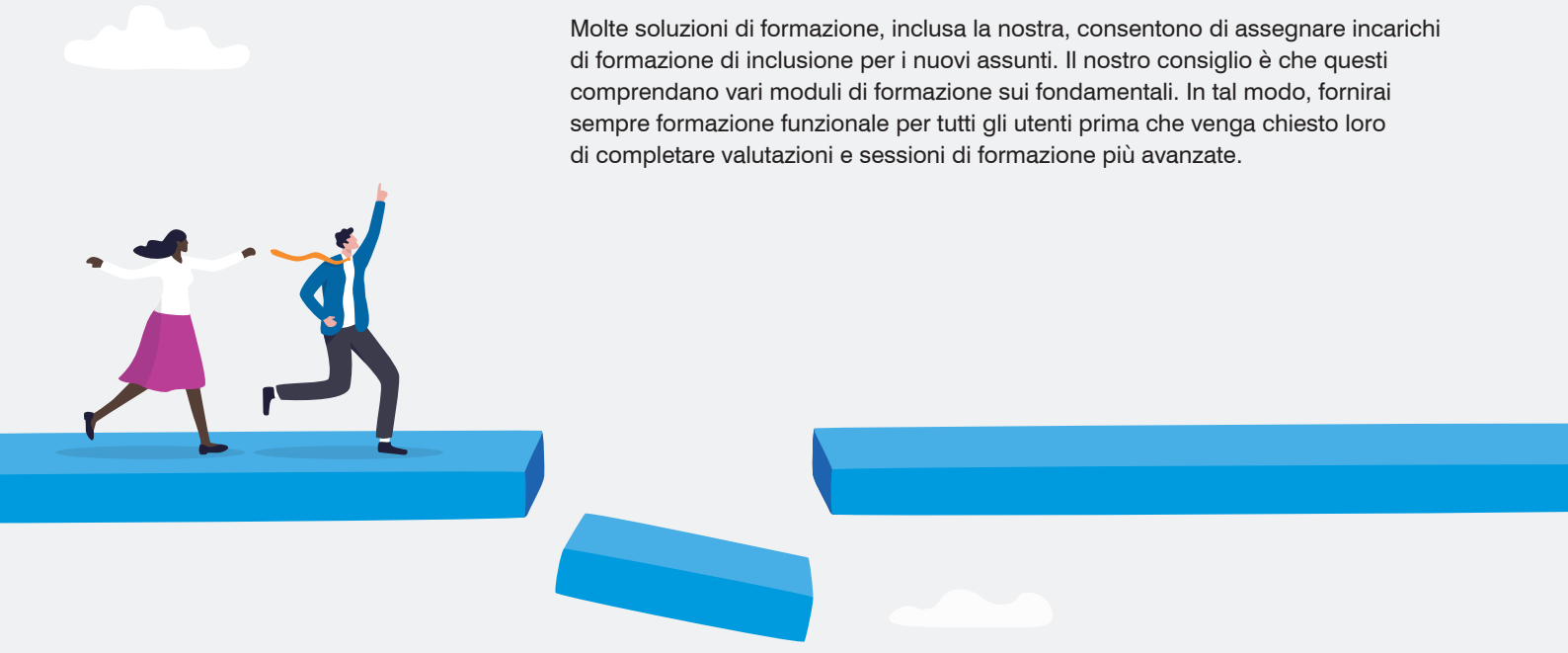
Nel nostro report State of the Phish 2020, abbiamo rilevato che molti adulti che lavorano non riescono a dare una definizione di termini quali phishing e ransomware.

	Corretto	Errato	Non so	
Cos'è il PHISHING?	61%	24%	15%	• Solo il 49% dei lavoratori statunitensi ha risposto correttamente. • I lavoratori tedeschi hanno riconosciuto più diffusamente questo termine (66%).
Cos'è il RANSOMWARE?	31%	31%	38%	• Lo scorso anno, il 45% dei lavoratori globali ha risposto correttamente a questa domanda. Questa diminuzione della consapevolezza potrebbe essere spiegata dal forte calo del numero di attacchi ransomware osservati nel 2018, il che significa che l'argomento è meno discusso nelle comunicazioni tra gli utenti e i team della sicurezza.

Fonte: State of the Phish 2020

Queste lacune nelle conoscenze sono il motivo per cui consigliamo caldamente la formazione funzionale su argomenti essenziali come le basi della sicurezza e il phishing prima di valutare o formare su argomenti più avanzati.

Molte soluzioni di formazione, inclusa la nostra, consentono di assegnare incarichi di formazione di inclusione per i nuovi assunti. Il nostro consiglio è che questi comprendano vari moduli di formazione sui fondamentali. In tal modo, fornirai sempre formazione funzionale per tutti gli utenti prima che venga chiesto loro di completare valutazioni e sessioni di formazione più avanzate.



Identificazione di utenti e VAP vulnerabili

Utilizzando il modello VAP che abbiamo descritto nell'introduzione, il tuo programma dovrebbe dare la massima attenzione agli utenti che rappresentano un rischio elevato perché:

- Sono particolarmente vulnerabili alle tattiche dei criminali informatici.
- Vengono presi di mira più frequentemente dagli attacchi.
- Hanno privilegi di accesso a dati, sistemi o risorse di valore.

(Consulta la sezione "Un modello incentrato sulle persone per la misurazione e la mitigazione del rischio utente" a pagina 3.)

Misurazione di vulnerabilità, attacchi e privilegi

Per le vulnerabilità, gli attacchi di phishing simulato e le valutazioni della conoscenza che utilizzano le domande sono irrinunciabili. Possono aiutarti a individuare gli utenti che hanno bisogno di approfondire la formazione, le tattiche che ingannano maggiormente gli utenti e gli ambiti da coprire.

Quantificare il rischio per l'utente nell'ambito del modello VAP ti consente di focalizzare il tuo programma di formazione e ridurre il rischio più rapidamente.

Per quanto riguarda gli attacchi, sapere quali sono gli utenti maggiormente presi di mira, come e da chi richiede informazioni utili fornite dalla soluzione di threat intelligence del team della sicurezza. Identifichiamo questi VAP tramite il nostro Attack Index, un punteggio composito che tiene conto dei seguenti fattori:

- **Tipo di criminale informatico.** Il livello di sofisticatezza dell'hacker e, di conseguenza, il rischio per l'azienda. Per esempio, l'autore di un attacco sponsorizzato da uno Stato riceve un punteggio molto più elevato di quello di un piccolo criminale informatico.
- **Tipo di presa di mira.** Un modo per descrivere con che precisione viene mirato l'attacco. La minaccia ha colpito un solo utente o ha avuto una portata globale? Era focalizzata su un utente, un'azienda, un settore o un'area geografica? Oppure era una campagna ad ampio spettro, lanciata contro mezzo mondo? Più mirata è la minaccia, più alto è il punteggio che le viene assegnato.
- **Tipo di minaccia.** Questo attributo indica il tipo di malware coinvolto nell'attacco. Nella maggior parte dei casi, il malware utilizzato in un attacco ci rivela la gravità della minaccia o l'entità dell'impegno profuso dal criminale informatico nel diffonderla. Un Trojan horse di accesso remoto, ad esempio, ottiene un punteggio più alto rispetto a un tentativo di phishing delle credenziali generico focalizzato sui clienti.

Riguardo al privilegio, le aziende possono iniziare a fare l'inventario di tutte le cose potenzialmente preziose a cui le persone hanno accesso, tra cui dati, autorizzazione finanziaria, relazioni chiave e molto altro.

La posizione di un utente nell'organigramma è naturalmente un fattore da tenere in considerazione nella valutazione dei privilegi, ma non è l'unico, anzi spesso non è neanche il più importante. Ai fini dello spionaggio industriale una segretaria potrebbe essere un bersaglio più invitante di un dirigente di medio livello, dal momento che la segretaria ha accesso al calendario dell'amministratore delegato. Allo stesso modo, un'infermiera di un ospedale autorizzata ad accedere ai record dei pazienti potrebbe essere un bersaglio più utile per dei ladri d'identità rispetto a un amministratore delegato.

Pratiche legate alle password

utilizza un gestore di password

sceglie a rotazione tra 5 e 10 password diverse

digita manualmente una password diversa per ogni accesso

utilizza sempre le stesse 1 o 2 password per tutti gli account

Fonte: State of the Phish 2020

Utilizzo dei dati VAP al di là della formazione

Quantificare il rischio per l'utente nell'abito del modello VAP ti consente di focalizzare il tuo programma di formazione e ridurre il rischio più rapidamente. Può anche fornire un contesto rispetto al perché i criminali informatici prendano di mira questi utenti. Con queste informazioni utili, puoi controllare più da vicino questi utenti e altri con ruoli analoghi e distribuire controlli adattivi come l'isolamento dell'attività del browser o l'incremento dei requisiti di autenticazione secondo necessità.

Combinando queste informazioni con la threat intelligence, per esempio, i dati forniti da uno strumento come Proofpoint Targeted Attack Protection (TAP), puoi stabilire con maggior precisione se gli utenti vengono presi di mira con contenuti dannosi.

Sapere se gli utenti fanno clic sulle email di phishing simulato è utile. Sapere se fanno clic su reali contenuti dannosi è ancora più importante, anche se il clic è bloccato e non ha conseguenze. Questi dati possono mettere in evidenza rischi potenziali e lacune.

Al di là del phishing: altre tematiche di sicurezza sensibili

Il phishing è l'argomento maggiormente dibattuto nella formazione per la sensibilizzazione alla sicurezza. La focalizzazione del programma esclusivamente sulle minacce basate su email può lasciare dei divari consistenti in altre aree di argomenti importanti.

Valuta l'impiego di una valutazione delle conoscenze ad ampio spettro per comprendere la conoscenza degli utenti sui temi della sicurezza informatica e sulle policy e linee guida della tua stessa azienda.

Il nostro report State of the Phish 2020 ha messo il luce una serie di comportamenti rischiosi. Alcuni esempi sono riportati di seguito:

- Il 45% degli adulti che lavorano ammette di utilizzare le stesse password per più account.
- Solo il 49% protegge la propria rete Wi-Fi di casa tramite password.
- Il 26% ritiene di potersi collegare in sicurezza a una rete Wi-Fi gratuita in un ambiente affidabile (ad esempio un internet café o un aeroporto).
- Il 17% non è sicuro che le reti ad accesso libero in questi ambienti siano sicure.

Tali comportamenti espongono la tua azienda a un grave rischio. Diversificare il programma per risolvere i problemi legati a queste e ad altre potenziali aree vulnerabili può ridurre la tua esposizione.

Quando affronti questi argomenti, utilizza esempi reali e coinvolgenti. Riferire dettagli pertinenti e concreti aiuta gli utenti a capire come si muovono i criminali informatici, e perché è importante capirlo.

Implementazione di un programma agile

Ogni azienda è associata a un panorama delle minacce, un bacino di utenti e una cultura della sensibilizzazione alla sicurezza unici. Così come è importante pianificare in anticipo, altrettanto lo è l'agilità.

Un programma agile si adatta alle mutevoli circostanze e si concentra sull'erogare la formazione alle persone giuste. Aiuta a garantire che il tuo programma sia completo, efficace ed efficiente. Infine, aiuta a ridurre il rischio utente sfruttando al meglio quelle poche ore all'anno che la maggior parte delle aziende riesce a dedicare alla formazione per la sensibilizzazione alla sicurezza.

I programmi più efficaci allineano gli esercizi di formazione alle minacce reali e potenziali. Adatta il programma in base alle circostanze. La vita è imprevedibile e i cambiamenti repentini possono creare nuovi divari di conoscenza e rischi per gli utenti.

Ecco alcuni esempi di situazioni in cui è possibile modificare il proprio piano in base alle esigenze o all'emergenza di nuove vulnerabilità.

- Le valutazioni di phishing dimostrano che gli utenti conoscono bene gli attacchi basati sui link ma hanno invece difficoltà a individuare gli attacchi che sfruttano gli allegati.
- La tua azienda viene presa di mira con un volume crescente di attacchi BEC (violazione dell'email aziendale).
- Il tuo team di sicurezza email osserva che i criminali informatici utilizzano un marchio specifico di inganno di phishing o di tipo di attacco.
- Nelle valutazioni della tua conoscenza, noti che un determinato reparto fatica a cogliere un argomento essenziale.

Automazione della formazione di follow-up

Automatizzare queste attività può rendere ancora più agili le tue attività. Ad esempio, i nostri clienti utilizzano la funzione di iscrizione automatica della nostra soluzione per assegnare automaticamente le sessioni di formazione in base al livello raggiunto dagli utenti negli attacchi simulati e nelle valutazioni delle conoscenze. La funzione indirizza la formazione verso gli utenti che ne hanno più bisogno ma non li obbliga a portarla a termine in quel momento.

Il follow-up automatico è un ottimo sistema per personalizzare la formazione in base alle reali vulnerabilità e lacune anziché adottare un approccio uguale per tutti che assegna la stessa formazione a tutti gli utenti. La formazione mirata fa risparmiare tempo agli utenti e viene accolta più volentieri dalle parti interessate.

Possibilità di "esonero" per gli utenti

Un altro metodo per personalizzare la formazione è consentire agli utenti di provare dimostrando che capiscono i concetti di sicurezza informatica e sanno tenere un buon comportamento. Se gli utenti hanno seguito la formazione di base, respingono (o segnalano) regolarmente le simulazioni di attacchi di phishing e ottengono buoni risultati nelle valutazioni della conoscenza, non hanno bisogno di seguire tutti i corsi di formazione.

Questa possibilità di esonero potrebbe aiutare gli utenti ad accogliere più favorevolmente la formazione e dare loro un incentivo per partecipare in modo più consapevole alle valutazioni.

SEZIONE 5

Parametri che contano: la misura del successo del programma

Se gestisci un programma di sensibilizzazione alla sicurezza, conosci probabilmente il significato di tasso di clic, noto anche come tasso di insuccesso. È la prima e la più importante statistica a essere citata dagli utenti che cercano di misurare l'efficacia del loro programma. E ovviamente è importantissimo da rilevare.

Tasso di segnalazione

Ma non è l'unico parametro di cui devi tenere conto. Misurare le percentuali in base alle quali gli utenti segnalano attivamente le email dannose (reali e simulate) può fornire indicazioni importanti.

I componenti aggiuntivi di segnalazione email consentono agli utenti di mettere facilmente in guardia il proprio team di sicurezza rispetto alle email sospette. Questi strumenti sono anche in grado di misurare quanti utenti che ricevono email di phishing simulato le segnalano; tale parametro è noto come tasso di segnalazione.

Sfortunatamente, solo il 15% delle aziende utilizza questi strumenti nel proprio programma di sensibilizzazione alla sicurezza informatica, secondo il nostro sondaggio State of the Phish 2020.

I nostri dati hanno individuato una maggiore variabilità nel tasso di segnalazione rispetto ai tassi di clic, come a indicare che il primo è un indicatore complessivamente più accurato del cambiamento di comportamento.

* Era consentito dare più risposte.

Fonte: State of the Phish 2020

Livelli di conoscenza

Un'altra fonte di indicazioni utili sono i livelli di conoscenza. Click rate e tasso di segnalazione sono in grado di misurare la resilienza degli utenti agli attacchi di phishing. Ma le valutazioni della conoscenza misurano la loro capacità di comprendere altri argomenti quali privacy dei dati, password e sicurezza dei dispositivi mobili.

Le aziende o i dipartimenti rigidamente regolati possono ad esempio richiedere formazione specifica. Comprendere i livelli di conoscenza degli utenti, e il loro andamento in crescita o in calo, è fondamentale.

Confronto tra tassi di clic e di segnalazione

Se si invia un'email di phishing simulato, quale può essere considerato un "buon" tasso di clic? La risposta dipende da due fattori principali:

- Quando è difficile e mirata l'email di phishing simulato
- Qual è il grado di competenza degli utenti

In generale, tassi di clic (o tassi di insuccesso) inferiori al 5% sono considerati buoni. Tuttavia, una misura più precisa riguarda lo scarto (superiore o inferiore) del tasso di insuccesso medio registrato in un'ampia gamma di aziende.

Proofpoint, insieme a molti altri fornitori, fornisce il tasso di insuccesso medio di modelli diversi di simulazioni di attacchi di phishing. Come mostra lo screenshot seguente, un tasso di insuccesso del 5% corrisponde a un risultato inferiore alla media per alcuni modelli.

In generale, tassi di clic (o tassi di insuccesso) inferiori al 5% sono considerati buoni.

Confronto dei tassi medi di insuccesso del nostro prodotto ThreatSim® (in verde).

Jump in this quick meeting	Corporate	8%
FREE GDPR Readiness Tools - Targets Legal or HR	Commercial	3%
College Admissions Help	Consumer	2%
Online dating - Message waiting	Proofpoint - Consumer	5%

Ecco perché il confronto dei tuoi risultati con questi tassi di insuccesso fornisce maggiori indicazioni sulla sensibilizzazione al phishing degli utenti. I tassi di insuccesso possono cambiare nel tempo, man mano che sempre più aziende adottano determinati modelli.

Per i tassi di segnalazione (utenti che riconoscono che un'email di phishing simulato è sospetta e la segnalano) si punta al 70%. Diversi dei nostri clienti hanno raggiunto tassi di segnalazione maggiori dell'80%, oltre a bassi tassi d'insuccesso.

Misurazione dell'impatto

I parametri di sensibilizzazione alla sicurezza sono importanti e accedervi dovrebbe essere facile nell'ambito del software di sensibilizzazione alla sicurezza. Ma il vero obiettivo di qualsiasi programma di formazione per la sensibilizzazione alla sicurezza è la riduzione del rischio utente.

A tal fine, i parametri esterni possono consentire di valutare e dimostrare il valore del tuo programma. Le misure chiave comprendono:

- Numero di infezioni malware e ripristini delle macchine utente.
- Tempo e risorse dedicati alla gestione della casella di posta per gli abusi.
- Numero di attacchi di phishing in circolazione riusciti.
- Downtime per gli utenti.

Questi parametri possono anche consentirti di mantenere l'accoglienza per il tuo programma da parte delle principali parti interessate. Uno dei nostri clienti ha risparmiato 345.000 dollari in spese legate al personale utilizzando un componente della nostra soluzione Proofpoint Closed-Loop Email Analysis and Response (CLEAR). (Ulteriori informazioni al riguardo nel report Forrester "The Total Economic Impact Of Proofpoint Advanced Email Protection", L'impatto economico totale della soluzione Proofpoint di protezione avanzata dell'email).)

Uno dei nostri clienti ha risparmiato

345.000$

in spese del personale utilizzando un componente della nostra soluzione CLEAR.

Uso dei tuoi dati per orientare la conversazione

Molti dei parametri utilizzati per parlare della formazione per la sensibilizzazione alla sicurezza (tasso di insuccesso, di clic, ecc.) possono avere connotazioni negative e sottolineare gli errori anziché i successi. Altri parametri, come i tassi di segnalazione e i livelli di conoscenza, mettono l'accento sul comportamento positivo rispetto a quello negativo. Inoltre, mostrano con maggiore accuratezza le prestazioni degli utenti come linea di difesa contro gli attacchi mirati di oggi.

Utilizza questi dati per raccontare le testimonianze di successo sui modi in cui gli utenti si stanno impegnando per migliorare la posizione di sicurezza della tua azienda. Supponi che un utente abbia segnalato un messaggio realmente dannoso e che il tuo team di risposta agli incidenti sia stato in grado di rimuoverlo prima che mettesse a rischio la tua azienda. Testimonianze come queste possono agevolare la vendita interna di programmi alle principali parti interessate e migliorare la cultura della sicurezza della tua azienda.

SEZIONE 6

Oltre la formazione: come creare una cultura della sicurezza informatica

Quasi il 99% delle aziende dichiara di proporre ai propri collaboratori una formazione di sensibilizzazione al phishing[2]. Ma il 43% forma solo una parte del proprio personale. Non stupisce quindi che il phishing resti il tipo di minaccia con più probabilità di causare una violazione dei dati.

Come migliorare la situazione? Creando una cultura della sicurezza sistematica, sostenibile e personalizzata che copre tutta l'azienda, dagli utenti alle attività digitali.

Questo approccio richiede un investimento concertato di tempo, sforzi, risorse e supporto in tutta l'impresa. Ma i benefici sono inestimabili. Una solida cultura della sicurezza informatica può migliorare il livello di sicurezza, la conformità e i risultati operativi della tua azienda. Può anche aumentare la fiducia e la produttività dei tuoi collaboratori.

2 Proofpoint. "State of the Phish 2022.", Febbraio 2022.

Cos'è una cultura della sicurezza informatica?

Secondo i ricercatori del MIT Keman Huang e Keri Pearlson la cultura della sicurezza informatica rappresenta "le convinzioni, i valori e le attitudini che motivano gli utenti a proteggere e difendere la loro azienda dagli attacchi informatici"[3].

In altre parole, tutti i collaboratori, senza eccezioni, sono agenti attivi per la difesa di dati, sistemi e risorse aziendali.

Per creare una cultura della sicurezza informatica è necessario riuscire a cambiare il modo di pensare dei collaboratori riguardo a tale argomento. La cultura della sicurezza informatica deve essere parte integrante della sicurezza aziendale. Deve ispirare e durare nel tempo.

Cosa forma una cultura?

Una cultura della sicurezza informatica comprende tre fattori sovrapposti:

- **Responsibilità per la sicurezza informatica.** I collaboratori si sentono responsabili, individualmente e collettivamente, delle loro azioni per prevenire gli incidenti di sicurezza.
- **Comprensione dell'importanza della sicurezza informatica.** I collaboratori sono consapevoli che le minacce informatiche rappresentano un rischio importante per il successo dell'azienda e possono avere ripercussioni su di loro.
- **Capacità di agire.** I collaboratori diventano più autonomi grazie alle loro conoscenze in materia di sicurezza informatica, alla comprensione delle policy di sicurezza e alla certezza che l'azienda li sosterrà se commettono un errore involontario relativo alla sicurezza.

Caratteristiche di una solida cultura della sicurezza informatica

Una solida cultura della sicurezza informatica presenta le seguenti caratteristiche:

- **Globalità e continuità.** La cultura della sicurezza non deve limitarsi alla formazione o a simulazioni di phishing sporadiche. L'obiettivo è quello di promuovere un clima di fiducia tra tutti i collaboratori per aumentare il loro coinvolgimento e migliorare il loro comportamento in materia di sicurezza. A tal fine si possono utilizzare molti modi. Una cultura della sicurezza informatica promuove l'apprendimento e la sensibilizzazione tramite contenuti pertinenti e personalizzati e il monitoraggio dell'evoluzione del panorama delle minacce. Gli utenti ricevono email e altri promemoria che li aiutano a capire perché stanno partecipando al programma e in che modo possa essere utile alla loro vita professionale e personale. Sono incoraggiati a segnalare in modo confidenziale gli eventi digitali sospetti.
- **Portavoce privilegiati trasversali.** Questi portavoce assicurano la trasmissione tra il team dirigenziale e gli utenti finali, attraverso i quadri intermedi. Oltre alla dirigenza, i "sostenitori" possono provenire da altri dipartimenti tra cui sicurezza, IT, risorse umane, conformità e audit, marketing e pubbliche relazioni[4].
- **Creazione e supporto delle aspettative.** Ciò implica la creazione e l'applicazione di policy di sicurezza che supportino le norme culturali.

3 Keman Huang e Keri Pearlson (MIT). "For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture" (Creare un modello di cultura della cybersecurity in azienda per affrontare le lacune tecnologiche), gennaio 2019.
4 SANS Institute. "2021 Security Awareness Report: Managing Human Cyber Risk" (Report 2021 sulla sensibilizzazione alla sicurezza informatica: gestire il rischio informatico umano), novembre 2021.

I vantaggi

Una solida cultura di sensibilizzazione alla sicurezza informatica può avere effetti positivi sulla missione dell'azienda e fornire vantaggi rilevanti e misurabili. Ecco alcuni esempi:

Miglioramento dell'agilità e della resilienza

Una cultura della sicurezza stimola gli utenti a riconoscere le potenziali minacce. Inoltre, consente ai team della sicurezza di reagire e di neutralizzarle più velocemente. L'agilità e la resilienza aumentano quando gli utenti sono motivati, vengono coinvolti e si sostengono a vicenda per fare rete. I benefici si amplificano in tutta l'azienda.

Riduzione dei rischi per l'azienda

Viviamo in un'epoca di cambiamenti, con il passaggio al telelavoro e al lavoro ibrido, la migrazione al cloud e il crescente utilizzo di dispositivi personali. I rischi si moltiplicano. Una solida cultura della sicurezza contribuisce a rassicurare i dirigenti, che possono così concentrarsi su altre attività.

Conformità senza problemi

La conformità con le normative ufficiali, gli standard del settore e le policy di sicurezza interne risulta più facile, con conseguente riduzione del rischio di incorrere in multe e altre sanzioni.

Vantaggio competitivo

Clienti e partner sceglieranno la tua azienda rispetto ai concorrenti se si sentiranno più sicuri. Promuovi la sicurezza come valore fondante.

Ostacoli comuni

Le aziende spendono milioni in strumenti, servizi e personale di sicurezza, ma nonostante tali investimenti, molte di esse trascurano il fattore di rischio più importante: i collaboratori.

Affrontare il fattore umano è la prima misura di sicurezza da implementare. È anche la più complicata. I programmi di sensibilizzazione possono essere destabilizzanti e fonte di distrazione. Alcuni collaboratori ritengono che impediscano loro di svolgere correttamente il loro lavoro. Molti sono riluttanti a svolgere compiti aggiuntivi, come la segnalazione di email sospette o la partecipazione a webinar di formazione. Inoltre, il personale tecnico e le risorse umane possono essere riluttanti a implementare una cultura della sicurezza informatica poiché non hanno le risorse per crearla e mantenerla viva.

Sfide principali:

- Far accettare l'idea ai dirigenti
- Quantificare in modo convincente il ritorno sull'investimento
- Convincere gli utenti dei vantaggi della formazione e sensibilizzazione alla sicurezza informatica e farli partecipare attivamente
- Modificare il comportamento dei collaboratori

Dalla teoria alla pratica con il framework ACE

La motivazione è fondamentale per generare una solida cultura della sicurezza informatica, basata su tre elementi chiave: Il primo è l'autonomia. Ogni utente deve ricevere una formazione personalizzata e autogestita. Il secondo è la padronanza. Devi mettere a disposizione degli utenti gli strumenti e il tempo necessari per progredire e sviluppare le loro conoscenze e competenze in materia di cybersecurity. L'ultimo ingrediente è la finalità. I tuoi utenti devono sentirsi parte di una missione che va oltre la loro funzione.

Utilizzo del framework ACE

La creazione di una cultura della sicurezza informatica sostenibile prevede tre fasi. Si tratta di un processo continuo, che definiamo framework ACE.

A Analizzare la vulnerabilità degli utenti

Ogni azienda è unica, con i suoi rischi e le sue priorità di sicurezza.

Poniti le seguenti domande:

- Qual è il livello di conoscenza dei tuoi utenti?
- Chi tra loro viene preso di mira? Da quali tipi di attacco?
- Come reagirebbero questi utenti di fronte alle minacce?
- Cosa credono? Cosa pensano della sicurezza informatica?

Queste e altre domande ti aiuteranno a identificare i tuoi punti deboli.

C Cambiare i comportamenti

La creazione di una cultura della sicurezza informatica è un processo continuo, non un singolo evento. Adotta un approccio olistico

comunicando regolarmente con i tuoi collaboratori, tramite molteplici canali di comunicazione, tra cui newsletter periodiche, blog interni e aggiornamenti sulle ultime minacce e i vettori d'attacco.

Varia e personalizza i contenuti. Ogni utente è unico, per cui reagisce e apprende in modo differente. Ricorda di rafforzare continuamente in modo positivo l'importanza della sicurezza.

E Valutare i progressi e monitorare il successo

Condividi i parametri che mostrano i progressi, il miglioramento continuo e il ritorno sull'investimento. Questi parametri quantificabili giustificano il tuo investimento e dimostrano il valore della cultura della sicurezza informatica alla dirigenza e all'azienda nel suo complesso.

Non perdere nemmeno un'opportunità. Dopo un attacco, mostra come una cultura della sicurezza informatica più solida avrebbe ridotto i tempi, i costi e l'impegno necessario per risolvere un incidente o aiutato l'azienda a evitarlo del tutto.

Esistono diversi modi per misurare il livello di sensibilizzazione alla sicurezza informatica della tua azienda e, quindi, di valutare il cambiamento del comportamento degli utenti indotto dalla tua cultura della sicurezza.

Per esempio:

- Tasso di clic degli utenti più vulnerabili
- Tasso di segnalazione delle simulazioni di attacchi di phishing
- La precisione nell'identificazione delle minacce reali da parte degli utenti

Perché è importante?

La creazione di una cultura della sicurezza informatica vivace offre vantaggi a tutti i tuoi utenti: dalla dirigenza agli utenti finali, passando dal team della sicurezza ai manager.

Ma non esiste un modello universale. Ogni azienda è diversa e ha esigenze uniche. Alcune di queste differenze sono specifiche dell'attività svolta dall'azienda, altre al settore in cui si opera. Ogni cultura della sicurezza informatica è determinata da una combinazione di fattori interni ed esterni.

La creazione di un programma duraturo, che ottenga consensi a tutti i livelli, aiuta a radicare la sensibilizzazione alla sicurezza informatica nei valori fondamentali della tua azienda. Una vera cultura della sicurezza non consiste in una semplice sessione di formazione una tantum. È una mentalità che guida le attività quotidiane, lavorative e personali.

Questa sezione rappresenta un'introduzione generale per la creazione di una cultura della sicurezza informatica.

Per un approfondimento sulle culture della sicurezza e sul framework ACE, scarica il nostro eBook *Oltre la formazione di sensibilizzazione: l'importanza di creare una cultura della sicurezza informatica sostenibile.*

SEZIONE 7

Conclusioni e raccomandazioni

L'obiettivo del tuo programma per la sensibilizzazione alla sicurezza deve essere quello di mettere in evidenza i comportamenti che sono più importanti per la missione della tua azienda. Il miglior modo per farlo è utilizzare una miscela di formazione ad ampio spettro e mirata che metta gli utenti in condizione di sapersi muovere grazie all'erogazione di consigli realizzabili.

Se non hai ancora adottato un approccio incentrato sulle persone nella formazione per la sensibilizzazione alla sicurezza informatica, è arrivato il momento di cominciare. Di seguito sono illustrati i cinque pilastri di un programma efficace ed efficiente:

Sviluppo di un programma incentrato sulle persone

Tutti i collaboratori in azienda possono essere un bersaglio. In qualsiasi momento, chiunque nella tua azienda può promuovere o danneggiare la tua posizione di sicurezza.

La formazione per la sensibilizzazione degli utenti è una delle operazioni più importanti che tu possa compiere per proteggere la tua azienda. Insegnando ai tuoi utenti a riconoscere, respingere e segnalare i tentativi di phishing, puoi creare una solida ultima linea di difesa contro le principali minacce informatiche di oggi.

Pianificazione dell'implementazione

Ogni azienda è unica e non esistono due programmi di formazione identici. Il tuo programma deve tuttavia includere i seguenti elementi:

- Definizione delle esigenze di formazione
- Individuazione degli utenti con esigenze formative specifiche
- Definizione delle attività
- Creazione e gestione dei programmi
- Comunicazione e verifica dei primi passaggi
- Definizione di frequenza e tempistica delle attività del programma

Maggiori sono la diligenza e la pianificazione che si applicano al programma e più il programma risulterà riuscito.

Coinvolgere gli utenti

Mantenere gli utenti impegnati è essenziale per un programma efficace. Ma anche i programmi con le migliori intenzioni possono diventare noiosi se non offrono un'esperienza significative e pertinenti.

I programmi più riusciti:

- Usano il branding per chiarire agli utenti quanto siano importanti.
- Adottano principi didattici scientificamente testati per modificare il comportamento.
- Rafforzano la formazione con un mix diversificato di contenuti e media.
- Reclutano sostenitori su tutta l'azienda per il supporto e i miglioramenti.
- Guidano gli utenti con il giusto equilibrio tra incentivi e conseguenze.

Uso dei dati per individuare utenti vulnerabili, focalizzare la formazione e restare agile

Le prime cose da fare dovrebbero essere fornire competenze di base, comprendere le vulnerabilità degli utenti e concentrare la formazione dove è maggiormente necessaria. In questo contesto, gli attacchi di phishing simulato e le valutazioni della conoscenza che utilizzano le domande sono indicazioni irrinunciabili per sapere dove concentrare le attività di formazione. Le informazioni di threat intelligence che forniscono indicazioni sugli attacchi a cui i tuoi utenti devono rispondere possono anche consentirti di allineare il contenuto della formazione alle minacce reali. Sapere quali utenti hanno accesso ai dati più sensibili di un'azienda può anche aiutarti a personalizzare la formazione e ad applicare controlli di sicurezza diversi agli utenti con privilegi elevati.

La formazione di follow-up automatica e le opzioni di esclusione per gli utenti esperti a basso rischio possono consentirti di restare agile su larga scala.

Misura il tuo successo con parametri interni ed esterni

I valori di click rate (o failure rate) per le email di phishing simulato sono importanti. I tassi di segnalazione delle email potrebbero tuttavia essere un'indicazione ancora più accurata di quanto gli utenti siano resilienti agli attacchi.

Le valutazioni delle conoscenze possono misurare la loro capacità di comprendere altri argomenti.

Infine, parametri esterni quali infezioni malware e downtime possono contribuire a mostrare effetto e valore del tuo programma.

Questi parametri possono anche consentirti di ottenere l'accoglienza favorevole continua per il tuo programma da parte delle principali parti interessate. Utilizza questi dati per sottolineare i modi in cui gli utenti si stanno impegnando per migliorare la posizione di sicurezza della tua azienda. Potrai così promuovere in modo più efficace il programma al tuo interno, ma anche rafforzare la cultura della sicurezza informatica della tua azienda.

Ulteriori informazioni

Per ulteriori informazioni sulla conoscenza dei tuoi utenti in materia di sicurezza informatica, punti di forza e punti deboli e come puoi promuovere il cambiamento del comportamento, sottoponiti alla nostra valutazione del rischio delle persone all'indirizzo proofpoint.com/it/people-risk-assessment.

Perché Proofpoint

Ogni giorno, analizziamo oltre:

2,6 MLD DI EMAIL	**49 MLD** DI URL	**1,9 MLD** DI ALLEGATI
1,7 MLD DI MESSAGGI MOBILE	**430 MIO** DI DOMINI WEB	**143,000** ACCOUNT SOCIAL MEDIA

Le nostre soluzioni sono state adottate da oltre:

- **75%** DELLE AZIENDE FORTUNE 100
- **60%** DELLE AZIENDE FORTUNE 1000
- **30%** DELLE AZIENDE FORTUNE GLOBAL 2000

- **8.000** GRANDI AZIENDE
- **200.000** PICCOLE IMPRESE

PER SAPERNE DI PIÙ

Per maggiori informazioni visita **proofpoint.com/it**.

INFORMAZIONI SU PROOFPOINT

Proofpoint è un'azienda leader nella cybersecurity e nella conformità, che protegge dai rischi il patrimonio più importante di un'azienda: le persone. Con una suite integrata di soluzioni basate su cloud, Proofpoint aiuta le aziende di tutto il mondo a bloccare le minacce mirate, a salvaguardare i propri dati e a proteggere gli utenti dagli attacchi IT. Aziende di ogni dimensione, tra cui il 75% delle Fortune 100, si affidano alle soluzioni di sicurezza e di conformità incentrate sulle persone di Proofpoint per mitigare i rischi di sicurezza veicolati via email, cloud, social media e web. Per ulteriori informazioni: **www.proofpoint.com/it**.

proofpoint.

0504-001-05-02 10/22