proofpoint

2025

Kit del mese di sensibilizzazione alla sicurezza informatica

Minacce incentrate sulle persone oltre la posta in arrivo

Una guida curata, della durata di un mese, per aumentare la consapevolezza sulla sicurezza informatica.

Ogni ottobre, il Mese della Sensibilizzazione alla Sicurezza Informatica è dedicato **a parlare con i tuoi dipendenti e clienti su come rimanere al sicuro, sia al lavoro che a casa**. Proofpoint sa che la tua pianificazione deve essere avviata il prima possibile. Inizia subito con questa campagna gratuita e con i relativi contenuti sulle minacce incentrate sulle persone.

Questa campagna gratuita di sensibilizzazione alla sicurezza, della durata di 4 settimane, è pensata per mettere in evidenza i nuovi attacchi mirati alle persone. **Ha l'obiettivo di aiutare i tuoi dipendenti a comprendere, riconoscere e prendere decisioni sicure quando si trovano ad affrontare minacce informatiche.**

Informazioni sull'argomento di quest'anno: Minacce incentrate sulle persone oltre la posta in arrivo

Con l'espansione dello spazio di lavoro digitale, aumentano le sfide della sicurezza incentrata sulle persone. Sebbene la posta elettronica rimanga il principale vettore di attacco, i criminali informatici stanno estendendo i loro attacchi ad altri canali, come Microsoft Teams, Slack, Zoom, LinkedIn e WhatsApp.

Una volta che i criminali informatici hanno compromesso un account, lavorano per rafforzare la loro posizione, evitare di essere scoperti e predisporre ulteriori fasi del loro attacco.

Ciò può includere l'esfiltrazione di dati, la distribuzione di ransomware o il furto di denaro. Anche se le persone possono credere di interagire con un'entità fidata su queste piattaforme, potrebbero farlo inconsapevolmente con un criminale informatico. Ecco perché è **importante riconoscere i nuovi vettori d'attacco e le tattiche di ingegneria sociale, così da proteggere se stessi e l'organizzazione.**

Il materiale di quest'anno illustra le migliori pratiche per identificare le minacce che colpiscono gli utenti via email e attraverso altri canali digitali. Inoltre, spiega le tattiche di impersonificazione e di frode nella catena di fornitura ,oltre all'impatto della compromissione degli account. È la scelta ideale per il Mese della Consapevolezza sulla Sicurezza Informatica, ma puoi utilizzarla in qualsiasi momento dell'anno.

©Proofpoint, Inc. 2025

Informazioni su questo kit

Proofpoint ha selezionato una raccolta di risorse formative gratuite dalla libreria di contenuti Proofpoint ZenGuide Security Awareness. Il kit contiene messaggi per facilitare la comunicazione e una cadenza per il lancio della campagna. Ti invitiamo a esaminare le nostre risorse consigliate, i messaggi della campagna e la tempistica prima di finalizzare l'approccio della tua campagna.

Risorse consigliate

Abbiamo selezionato contenuti chiave che spiegano le minacce emergenti di oggi e i modi in cui le persone possono difendersi. I video generano un grande coinvolgimento, quindi il kit di quest'anno include cinque moduli di formazione, tutti scelti tra i contenuti tempestivi che Proofpoint pubblica sulla base della nostra threat intelligence leader di settore.

1. **«Panoramica delle minacce: Phishing nelle app di messaggistica»**

   Panoramica di 4 minuti su come gli aggressori eseguono attacchi di phishing mirati tramite email e strumenti di comunicazione e collaborazione, come Microsoft Teams, Slack e Google Chat

2. **«È il momento di riflettere su... la catena di fornitura»**

   Breve panoramica per sensibilizzare sugli attacchi alla supply chain e prevenire le frodi dei fornitori

3. **«60 secondi per una migliore sicurezza: Che cos'è lo spoofing?»**

   Panoramica di 1 minuto sullo spoofing delle email, suggerimenti per identificare le email falsificate e su come gli aggressori utilizzano questa tattica di impersonificazione

4. **«Note di un esperto: Compromissione dell'email aziendale (BEC, Business Email Compromise)»**

   Video di 3 minuti di un esperto di Proofpoint Threat Research sul motivo per cui gli aggressori utilizzano le truffe BEC e come riconoscerle

5. **«Le persone più attaccate: Proteggere gli account»**

   Panoramica di 2 minuti su come e perché gli aggressori prendono di mira determinati individui per il loro accesso a dati privilegiati o alla rete, e su come riconoscere e comprendere i rischi associati alla compromissione dell'account

©Proofpoint, Inc. 2025

Pianificazione
Prima del lancio

Un mese prima

- Esamina le risorse e le comunicazioni che proponiamo e definisci cosa userai nella tua campagna.
- Identifica i canali di diffusione di contenuti e comunicazioni (per esempio email, canali di chat interni, un portale condiviso e/o un wiki interno).
- Condividi il piano con i principali stakeholder e decisori e correggi la rotta se necessario.
- Ottieni sponsorship dall'alto e collaborazione trasversale per amplificare la voce della campagna.
- Definisci data di lancio, data di chiusura e tappe intermedie.

Crea un repository centrale dei contenuti.

Ti suggeriamo un repository centrale, come un wiki interno, per tutte le risorse formative rivolte agli utenti. In questo modo non dovrai inviare tutti i contenuti via email o chat e i dipendenti avranno un unico punto di accesso per gestire la maggior parte delle attività assegnate.

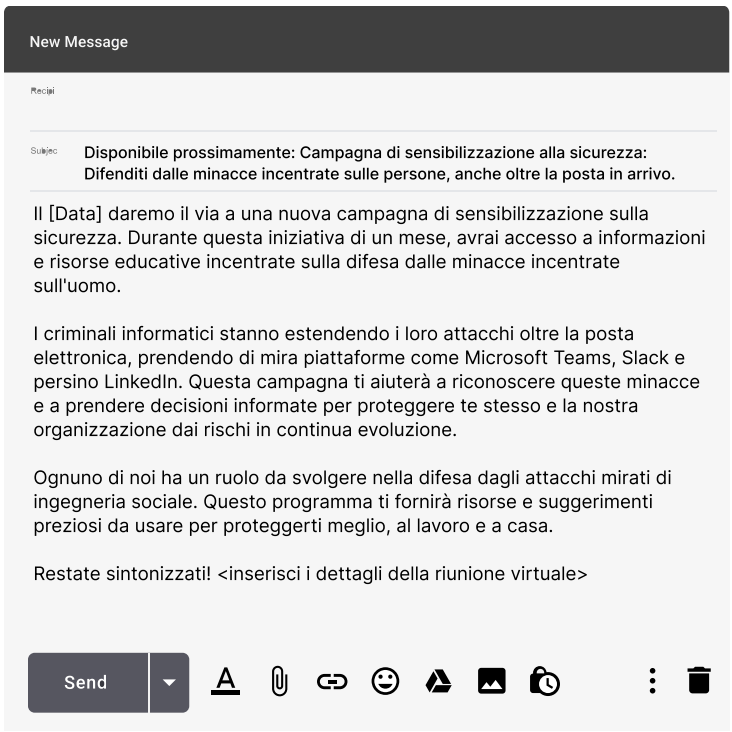
Crea un canale di chat interno

Se non l'hai già fatto, crea un canale dedicato alla sensibilizzazione e alla formazione sulla sicurezza informatica. Offre un modo rapido e semplice per inviare promemoria sulle attività del programma e sulle date fondamentali.

Una settimana prima

- Annuncia la prossima campagna
- La settimana precedente al lancio ufficiale, prepara un messaggio per tutti i membri della tua organizzazione. Ti consigliamo di inviare un'email a tutta l'organizzazione per presentare in anteprima il programma in arrivo. Se possibile, l'email dovrebbe provenire dal CISO o dal CEO della tua organizzazione. per dare peso e credibilità alla campagna, contribuendo a massimizzare i tuoi sforzi.

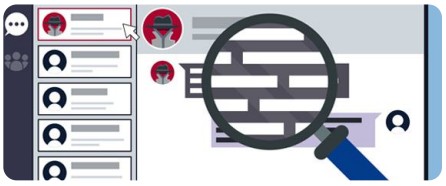
Invia questa comunicazione suggerita tramite e-mail o chat interna (modificala se necessario).



©Proofpoint, Inc. 2025

Avvio: Settimana 1

- Organizza una sessione di kickoff.
- Informa i partecipanti che riceveranno email settimanali con link ai moduli di formazione dedicati alla sicurezza.
- Nel tuo repository di contenuti, aggiungi il modulo video **«Panoramica delle minacce: Phishing nelle app di messaggistica.»**



Scarica risorse

Invia una comunicazione via email o chat interna utilizzando il testo suggerito qui di seguito (da modificare se necessario):

New Message

Recipients

Subject Phishing oltre la casella di posta

Le misure tecniche non possono sempre proteggerci, quindi è importante conoscere il nostro ruolo nel garantire la sicurezza. Guarda questo video di 4 minuti: "Panoramica delle minacce". "Phishing nelle app di messaggistica": scopri come gli aggressori lanciano attacchi di phishing anche oltre la posta elettronica, sfruttando Microsoft Teams, Slack, Google Chat e altri strumenti di messaggistica.

Impara a identificare un messaggio dannoso diffuso attraverso gli strumenti di comunicazione e collaborazione di uso quotidiano e ricorda: non tutti i canali dispongono di controlli di sicurezza tradizionali. Resta vigile e non cadere nella trappola!

Accedi al video al seguente link non appena ti è possibile. Guardalo per ottenere il massimo dal resto del materiale che condivideremo questo mese.

<[insert link]>

Send

Incoraggiare: Settimana 2

- Incoraggia la partecipazione all'inizio della seconda settimana
- Aggiungi il modulo video **«È il momento di riflettere su:»** La catena di fornitura

Scarica risorse

Invia una comunicazione via email o chat interna utilizzando il testo suggerito qui di seguito (da modificare se necessario):

New Message

Recipients

Subject È il momento di riflettere su: La catena di fornitura

Ormai dovresti aver guardato il video di sensibilizzazione che abbiamo condiviso la scorsa settimana (Se non l'hai ancora fatto, fallo oggi stesso!)

Oggi guarderemo un breve video: "Time to Think About: La "catena di fornitura" per ricordare l'importanza di essere consapevoli degli attacchi alla catena di fornitura. Il tema è la frode dei fornitori e mette in evidenza il rischio
che account compromessi possano essere sfruttati per colpire le relazioni commerciali di fiducia.

<[inserisci collegamento]>

Send

©Proofpoint, Inc. 2025

Complimenti: Settimana 3

- All'inizio della terza settimana, aggiungi due moduli video: **«60 secondi per una migliore sicurezza: Cos'è lo spoofing?»** (Settimana 3, Parte 1)
- **«Note di un esperto: Compromissione della posta elettronica aziendale.»**(Settimana 3, Parte 2)

Scarica risorse

Invia una comunicazione via email o tramite i canali di chat interni utilizzando il testo seguente (modifica se necessario).

New Message

Recipients

Subject 60 secondi per una migliore sicurezza: Che cos'è lo spoofing?

Congratulazioni a tutti coloro che stanno sfruttando al meglio il materiale di sensibilizzazione alla sicurezza informatica di questo mese.

Abbiamo aggiunto una nuova risorsa a <[inserisci collegamento]>: “60 secondi per una migliore sicurezza: Che cos'è lo spoofing?” Questo video offre una spiegazione di base dello spoofing delle email: quando un attaccante falsifica un indirizzo di invio affinché il messaggio sembri provenire da un’azienda, istituzione o persona legittima. Questa è una delle numerose tattiche di impersonificazione utilizzate dagli aggressori per indurre una persona a rivelare credenziali, informazioni finanziarie o dati personali.

Send

- **Più avanti nella settimana,** condividi un secondo video, Settimana 3, Parte 2, **«Note di un esperto: Compromissione della posta elettronica aziendale (BEC)»**.

Scarica risorse

Invia una comunicazione via email o tramite i canali di chat interni utilizzando il testo seguente (modifica se necessario).

New Message

Recipients

Subject Note di un esperto: Compromissione dell'email aziendale

Congratulazioni per i progressi compiuti nella terza settimana del materiale di sensibilizzazione sulla sicurezza informatica di questo mese.

Abbiamo aggiunto una nuova risorsa a <[inserisci collegamento]>: “Note di un esperto: Compromissione dell'email aziendale In questo video ascolterai un esperto di Proofpoint Threat Research parlare degli attacchi Business Email Compromise (BEC), spesso associati a email contraffatte e a tentativi di ingannare dipendenti, partner o clienti affinché trasferiscano denaro o divulghino dati sensibili.

Send

©Proofpoint, Inc. 2025

Riepilogo: Settimana 4

- All'inizio di quest'ultima settimana, aggiungi il modulo video **«Persone molto attaccate: Protezione degli account»**
- Invia una comunicazione per ricordare ai dipendenti di completare tutte le attività con un invito a una riunione virtuale di chiusura.

Scarica risorse

Invia una comunicazione via email o tramite i canali di chat interni utilizzando il testo seguente (modifica se necessario).

New Message

Recipients

Subject Protezione contro la compromissione dell'account

Ci auguriamo che abbiate tratto vantaggio dalle risorse di sensibilizzazione sulla sicurezza che abbiamo condiviso con voi questo mese. Per concludere, abbiamo aggiunto un ultimo video "Persone molto attaccate: Protezione degli account." <[inserisci collegamento]> Sono due minuti interessanti su come e perché gli aggressori prendono di mira determinati individui che hanno accesso a dati sensibili o privilegiati in rete, e su come riconoscere e comprendere i rischi associati alla compromissione dell'account.

Vorrei anche invitarvi a un incontro virtuale conclusivo, durante il quale discuteremo delle storie di successo legate a questa campagna, celebreremo i partecipanti e raccoglieremo i vostri preziosi contributi.. <insert meeting details>

Per qualsiasi domanda o commento, non esitate a contattarmi all'indirizzo <[email]>.

Send

È il momento di concludere la campagna di sensibilizzazione sulla sicurezza informatica! Se possibile, aprite la discussione su punti importanti come i seguenti:

- Cosa è piaciuto e cosa non è piaciuto ai partecipanti della campagna
- Cose apprese che prima non si sapevano
- Argomenti su cui le persone vorrebbero saperne di più

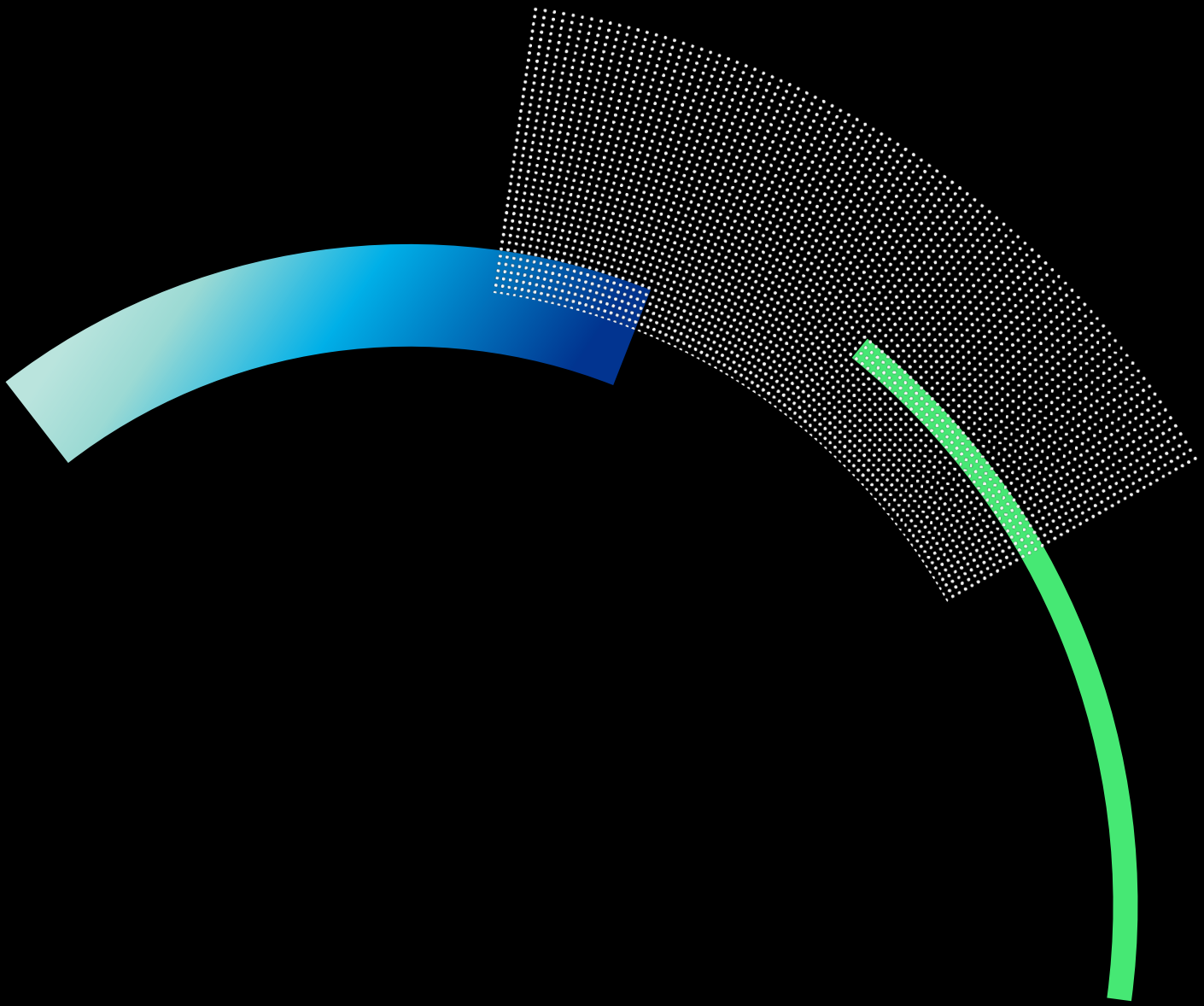
Questo kit vi aiuterà a dare il via al mese di sensibilizzazione sulla sicurezza informatica e a responsabilizzare i vostri dipendenti affinché siano più resilienti contro attacchi mirati alle persone, multicanale e multifase

Per un impatto maggiore

Diventa cliente Proofpoint e ottieni l'accesso completo alla libreria di contenuti ZenGuide™. Proofpoint ZenGuide è
una soluzione per aumentare la consapevolezza sulla sicurezza e promuovere comportamenti più sicuri. È un componente chiave di Proofpoint Prime Threat Protection, una soluzione completa e integrata che unisce tecnologia e formazione per offrire protezione e resilienza contro le attuali minacce informatiche incentrate sulle persone.

SCOPRI DI PIÙ SU PROOFPOINT PRIME THREAT PROTECTION →

©Proofpoint, Inc. 2025



proofpoint.

Proofpoint, Inc. 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 l'85% 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. UlteMaggiori informazioni sono disponibili sul sito https://www.proofpoint.com/it.

Connettiti con Proofpoint: Proofpoint è un marchio registrato o nome commerciale di Proofpoint, Inc. negli Stati Uniti e/o negli altri Paesi. Tutti gli altri marchi qui menzionati appartengono ai rispettivi proprietari.

SCOPRI LA PIATTAFORMA PROOFPOINT →