proofpoint

2025

Kit du mois de sensibilisation à la cybersécurité

Menaces centrées sur l'humain au-delà de la boîte de réception

Un guide structuré sur un mois pour renforcer la sensibilisation à la cybersécurité.

Chaque année en octobre, le Mois de la sensibilisation à la cybersécurité est dédié à **discuter avec vos employés et clients de la sécurité, aussi bien au travail qu'à la maison.** Chez Proofpoint, nous savons que votre planification doit intervenir à un stade précoce. Démarrez rapidement grâce à cette campagne gratuite et à ses contenus sur les menaces centrées sur l'humain.

Cette campagne gratuite de quatre semaines est conçue pour mettre en lumière de nouvelles attaques ciblant les personnes. **Elle aide vos employés à comprendre, identifier et prendre de bonnes décisions lorsqu'ils sont confrontés à des cybermenaces.**

À propos du thème de cette année : Menaces centrées sur l'humain au-delà de la boîte de réception

À mesure que l'espace de travail numérique s'étend, les défis de sécurité centrés sur l'humain se multiplient. Si l'email reste le principal vecteur d'attaque, les cybercriminels investissent aussi d'autres canaux comme Microsoft Teams, Slack, Zoom, LinkedIn et WhatsApp. Une fois un compte compromis, ils renforcent leur emprise, évitent la détection et déroulent les étapes suivantes de leur attaque.

Cela peut se traduire par une exfiltration de données, un déploiement de ransomware ou un vol financier. Même si les utilisateurs pensent interagir avec une entité de confiance sur ces plateformes, ils peuvent en réalité échanger avec un acteur malveillant sans le savoir. C'est pourquoi **il est important pour eux de reconnaître les nouveaux vecteurs d'attaque et les tactiques d'ingénierie sociale, afin de s'assurer que ils peuvent se protéger eux-mêmes ainsi que l'organisation.**

Notre document de cette année détaille certaines des meilleures pratiques pour identifier les menaces qui ciblent les utilisateurs par e-mail et sur d'autres canaux numériques. Il sensibilise également aux tactiques d'usurpation d'identité et de fraude à la chaîne d'approvisionnement, et explique l'impact d'une compromission de compte. C'est un excellent choix pour le Mois de la sensibilisation à la cybersécurité, mais vous pouvez l'utiliser à tout moment de l'année.

À propos de ce kit

Proofpoint a sélectionné pour vous des ressources de formation gratuites issues de la bibliothèque Proofpoint Security Awareness. Le kit comprend des messages prêts à l'emploi pour faciliter la communication et une cadence pour le lancement de la campagne. Nous vous invitons à examiner nos ressources recommandées, les messages de campagne et le calendrier avant de finaliser votre approche.

Ressources recommandées

Nous avons sélectionné des contenus clés qui expliquent les menaces émergentes actuelles et la façon de s'en protéger. Les vidéos génèrent un excellent engagement. C'est pourquoi le kit de cette année propose cinq modules de formation, choisis parmi les contenus actualisés publiés par Proofpoint sur la base de notre veille sur les menaces leader du secteur.

1. **« Présentation des menaces : « Hameçonnage dans les applications de messagerie »**
   Présentation de 4 minutes sur la façon dont les attaquants mènent des attaques de phishing ciblées, aussi bien par email que via des outils de communication et de collaboration comme Microsoft Teams, Slack et Google Chat

2. **« Il est temps de réfléchir… à la chaîne d'approvisionnement »**
   Capsule express pour sensibiliser aux attaques de la chaîne d'approvisionnement et à la prévention de la fraude fournisseur

3. **«60 secondes pour une meilleure sécurité : Qu'est-ce que le spoofing ?»**
   Présentation d'1 minute sur le spoofing d'email, avec des conseils pour identifier les emails usurpés et comprendre cette tactique d'imitation

4. **« Notes d'un expert : « Compromission de la messagerie professionnelle (BEC) »**
   Vidéo de 3 minutes d'un expert de Proofpoint Threat Research : pourquoi les attaquants utilisent les escroqueries BEC et comment les reconnaître

5. **«Personnes souvent ciblées : Protection des comptes»**
   Présentation de 2 minutes expliquant pourquoi et comment certains individus sont ciblés en raison de leur accès à des données privilégiées ou au réseau, et comment reconnaître et comprendre les risques liés à la compromission de comptes

Préparation
Avant le lancement

Un mois avant

- Passez en revue nos ressources et modèles de communication pour décider de ce que vous utiliserez.
- Définissez vos canaux de diffusion (email, chats internes, portail partagé et/ou wiki).Partagez le plan avec les parties prenantes et ajustez-le si nécessaire.Obtenez une adhésion à la fois descendante et transverse pour amplifier la portée de la campagne.Fixez la date de lancement, la date de fin et les étapes clés intermédiaires.

Créez un référentiel central de contenus

Nous vous recommandons d'utiliser un référentiel central, tel qu'un wiki interne, pour regrouper toutes les ressources d'apprentissage destinées aux utilisateurs dans le cadre de la campagne. Cela vous évitera d'envoyer tous vos contenus par email ou via les canaux de chat et offrira à vos collaborateurs un point d'accès unique pour gérer l'essentiel des activités qui leur sont attribuées.

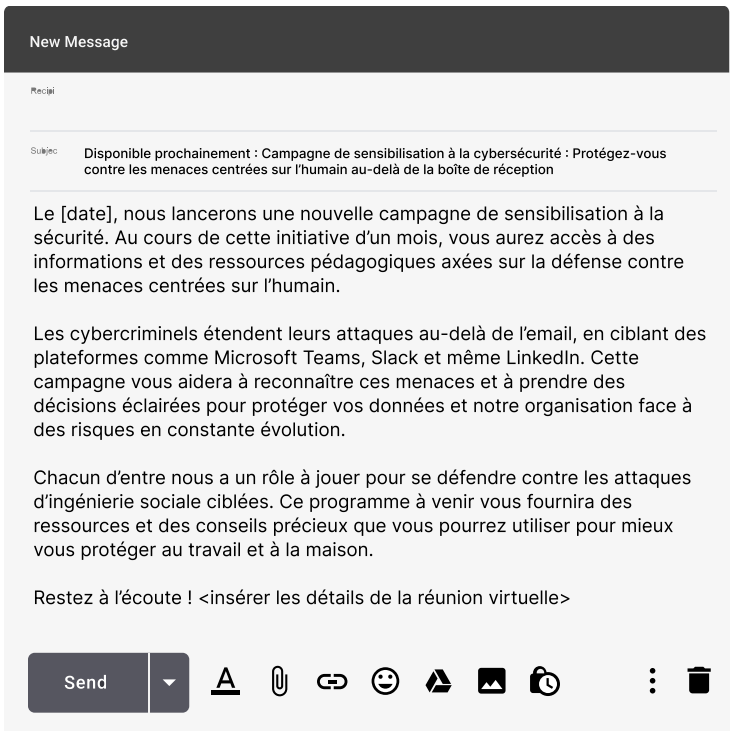
Créer un canal de chat interne

Si vous ne l'avez pas déjà fait, créez un canal de discussion interne spécialement conçu pour la sensibilisation et la formation en matière de cybersécurité. Cela offrira un moyen rapide et facile d'envoyer des rappels concernant les activités du programme et les dates clés.

Une semaine avant

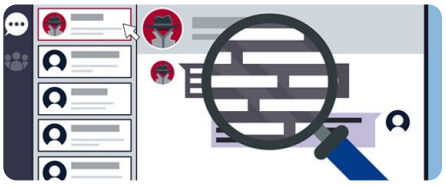
- Annoncez la campagne à venir
- La semaine précédant le lancement officiel, préparez un message à l'intention de l'ensemble de votre organisation. Nous recommandons d'envoyer un email à toute l'organisation pour présenter en avant-première le programme. Si possible, cet email doit être envoyé par le RSSI ou le PDG de votre entreprise. Vous apporterez ainsi du poids et de la crédibilité à la campagne, ce qui contribuera à maximiser vos efforts.

Envoyez cette communication suggérée par email ou via le chat interne (modifiez-la au besoin).



Lancement : Semaine 1

- Organisez une séance de lancement.
- Précisez aux participants qu'ils recevront des emails hebdomadaires avec des liens vers les modules de sensibilisation à la sécurité.
- Dans votre référentiel de contenus, ajoutez le module vidéo **« Présentation des menaces »** : Phishing dans les applications de messagerie.



Télécharger les ressources

Envoyez un message par email ou via le canal de chat interne en utilisant cette suggestion de texte (à modifier si nécessaire) :

New Message

Recipients

Subject Phishing au-delà de la boîte de réception

Les dispositifs techniques ne peuvent pas toujours nous protéger, il est donc important de connaître notre rôle pour rester en sécurité. Regardez cette vidéo de 4 minutes, « Présentation des menaces » : « Phishing dans les applications de messagerie », qui explique comment les attaquants mènent des attaques au-delà de l'email, via Microsoft Teams, Slack, Google Chat et d'autres outils de messagerie.

Apprenez à identifier un message malveillant diffusé dans les outils de communication et de collaboration du quotidien, et n'oubliez pas que tous les canaux ne disposent pas de contrôles de sécurité traditionnels. Restez vigilant et ne mordez pas à l'hameçon !

Accédez à la vidéo via le lien suivant dès que possible. Il est essentiel de la visionner pour tirer le meilleur parti des autres supports que nous partagerons ce mois-ci !
<[insérer le lien]>

Send

Encourager: Semaine 2

- Encouragez la participation dès le début de la semaine 2
- Ajoutez le module vidéo **« Il est temps de réfléchir: La chaîne d'approvisionnement. »**

Télécharger les ressources

Envoyez un message par email ou via le canal de chat interne en utilisant cette suggestion de texte (à modifier si nécessaire) :

New Message

Recipients

Subject Il est temps de réfléchir à : La chaîne d'approvisionnement

À ce stade, vous devriez avoir regardé la vidéo de sensibilisation que nous avons partagée la semaine dernière. (Si ce n'est pas le cas, faites-le dès aujourd'hui !)

Aujourd'hui, nous allons regarder une courte vidéo, "Il est temps de réfléchir à : « La chaîne d'approvisionnement », qui sert de rappel pour rester vigilant face aux attaques
visant la chaîne d'approvisionnement. Le sujet est la fraude fournisseur et met en évidence le risque
que des comptes fournisseurs compromis soient exploités pour cibler vos relations commerciales de confiance.

<[insérer le lien]>

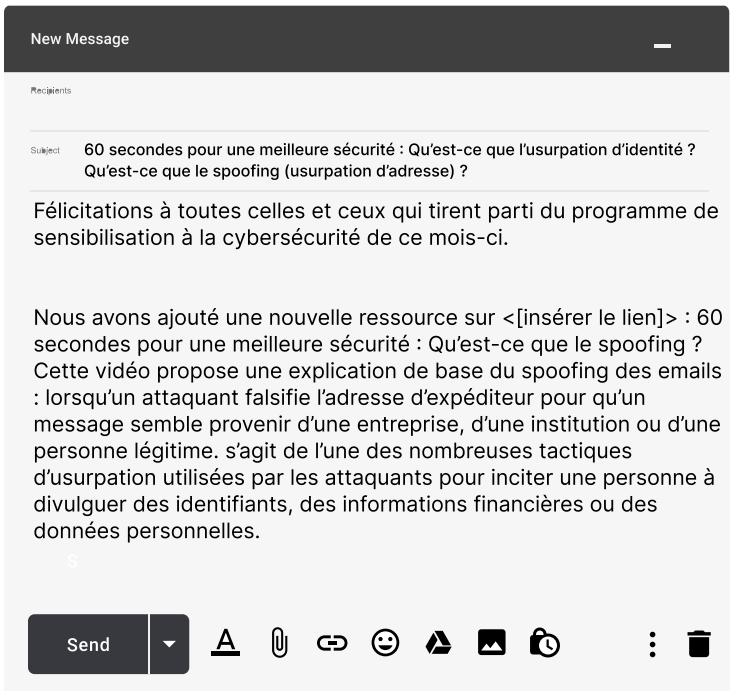
Send

Applaudir: Semaine 3

- Au début de la semaine 3, ajoutez deux modules vidéo : **«60 secondes pour une meilleure sécurité : Qu'est-ce que le spoofing (usurpation d'adresse) ? »** (Semaine 3, partie 1)
- **« Notes d'un expert : Compromission des e-mails professionnels.»** (Semaine 3, partie 2)

Télécharger les ressources

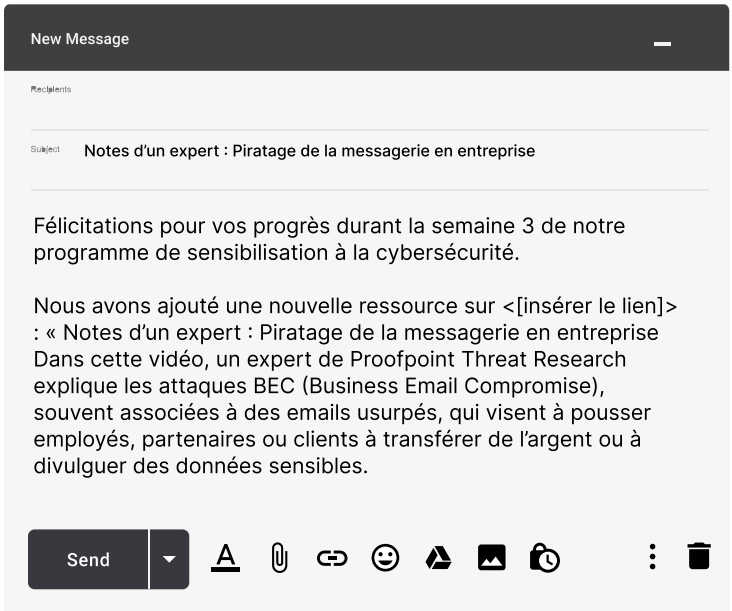
Envoyez une communication par email ou via vos canaux de chat internes en utilisant le texte ci-dessous (à adapter si nécessaire).



- Plus tard dans la semaine, partagez une deuxième vidéo, Semaine 3, partie 2, **« Notes d'un expert : Pertes dues aux attaques BEC : »**

Télécharger les ressources

Envoyez une communication par email ou via vos canaux de chat internes en utilisant le texte ci-dessous (à adapter si nécessaire).



Conclusion: Semaine 4

- Au début de cette dernière semaine, ajoutez le module vidéo **« Very Attacked Persons ». « Protéger les comptes »**
- Envoyez un message pour rappeler aux collaborateurs de finaliser toutes les activités et joignez une invitation à une réunion virtuelle de clôture.

Télécharger les ressources

Envoyez une communication par email ou via vos canaux de chat internes en utilisant le texte ci-dessous (à adapter si nécessaire).

New Message

Recipients

Subject Protection contre la compromission de compte

Nous espérons que vous avez tiré parti des ressources de sensibilisation à la sécurité partagées ce mois-ci. Pour conclure, nous avons ajouté une dernière vidéo « Very Attacked Persons » : « Protéger les comptes ». <[insérer le lien]>Une vidéo de deux minutes qui explique comment et pourquoi certaines personnes sont ciblées en raison de leur accès à des données sensibles ou au réseau, et comment reconnaître et comprendre les risques liés à la compromission de compte.

Je vous invite également à une réunion de synthèse virtuelle, où nous partagerons les réussites de la campagne, mettrons à l'honneur les participants et recueillerons vos retours. <insérer les détails de la réunion>

Pour toute question ou remarque, contactez-moi à <[email]>.

Send

Il est temps de conclure la campagne de sensibilisation à la cybersécurité ! Si possible, ouvrez la discussion sur des points importants tels que les suivants :

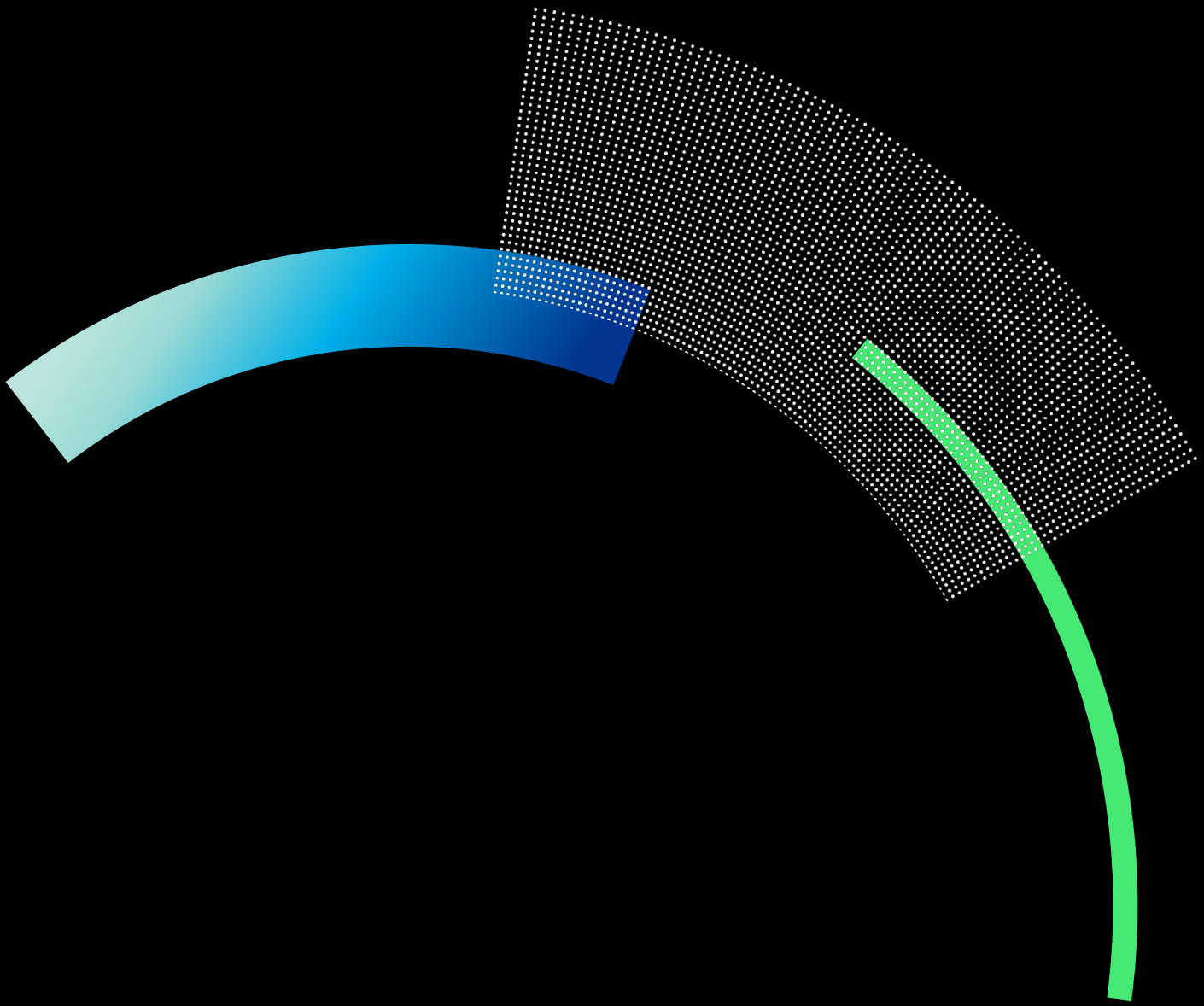
- Ce que les participants ont apprécié… et moins apprécié dans la campagne
- Ce qu'ils ont appris
- Les sujets sur lesquels ils souhaiteraient en savoir davantage

Ce kit vous aidera à lancer votre Mois de la sensibilisation à la cybersécurité et à rendre vos équipes plus résilientes face aux attaques centrées sur l'humain, multicanaux et en plusieurs étapes.

Vous voulez encore plus d'impact ?

Devenez client Proofpoint et bénéficiez d'un accès complet à la bibliothèque de contenus ZenGuide™. Proofpoint ZenGuide est une solution de sensibilisation à la sécurité qui favorise l'adoption de comportements plus sûrs. Il s'agit d'un composant clé de Proofpoint Prime Threat Protection, une solution complète et intégrée qui associe technologie et formation pour offrir protection et résilience face aux cybermenaces centrées sur l'humain d'aujourd'hui.

EN SAVOIR PLUS SUR PROOFPOINT PRIME THREAT PROTECTION →



proofpoint.

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risque des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris 85 % des entreprises du classement Fortune 100, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes pour diminuer leurs risques les plus critiques via la messagerie, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur :www.proofpoint.com/fr

Connectez-vous avec Proofpoint : LinkedIn

DÉCOUVRIR LA PLATEFORME PROOFPOINT →