proofpoint. | Protect people. Defend data.

GUIDE DE CAMPAGNE

Kit du mois de la sensibilisation à la cybersécurité 2024 : campagne « Détective en cybersécurité »

Guide sur un mois permettant de sensibiliser les utilisateurs au signalement des emails suspects à l'ère de l'IA

Chaque année en octobre, le mois de la sensibilisation à la cybersécurité est l'occasion de discuter avec vos collaborateurs et clients de leur sécurité, chez eux et au travail. Chez Proofpoint, nous savons que votre planification doit intervenir à un stade précoce. Lancez-vous en un rien de temps grâce à cette campagne et à ces contenus gratuits concernant les bonnes pratiques en matière d'identification et de signalement des emails de phishing.

À propos de notre thème

Les cybercriminels développent en permanence de nouvelles méthodes d'attaque. Une tactique demeure toutefois constante : les emails de phishing. Et avec l'avènement de l'IA générative, le phishing peut être encore plus difficile à identifier.

Vos collaborateurs sont amenés à recevoir des emails suspects qui les incitent à effectuer une action, comme cliquer sur un lien ou ouvrir une pièce jointe. Il est important qu'ils reconnaissent les signaux d'alerte et qu'ils sachent comment signaler ces emails.

Nous avons créé le thème « Détective en cybersécurité » spécialement pour cette campagne. Ensemble, nous passerons en revue les bonnes pratiques permettant d'identifier les messages suspects et de les signaler à votre entreprise. Cette campagne s'inscrit parfaitement dans le cadre du mois de la sensibilisation à la cybersécurité, mais vous pouvez l'utiliser à n'importe quelle période de l'année.

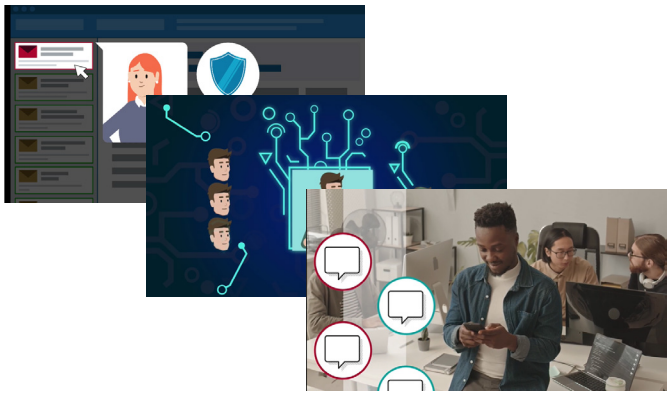
Comment utiliser ce kit

Proofpoint vous propose une sélection de ressources de formation gratuites issues de notre bibliothèque de contenus Proofpoint Security Awareness. Ces ressources vous aideront à apprendre aux utilisateurs à gérer les attaques de phishing, en particulier celles générées par l'IA. Le kit comprend des messages favorisant la communication, ainsi qu'une proposition de calendrier pour le déploiement de la campagne. Nous vous encourageons à examiner nos suggestions de ressources, de messages et de calendrier avant de finaliser votre campagne.

Suggestions de ressources

Vidéos

Nous avons sélectionné des ressources clés qui fournissent des informations sur différentes menaces de phishing et sur la façon dont les personnes peuvent se défendre. Les vidéos suscitent un engagement très fort. C'est pourquoi le kit 2024 comprend trois modules vidéo sélectionnés parmi les contenus publiés par Proofpoint en fonction de notre threat intelligence de pointe.



- **« Détective en cybersécurité : signalement des emails suspects »** – Vidéo de 2 minutes sur le thème du détective présentant les principes de base des emails de phishing et expliquant comment les reconnaître et s'en protéger
- **« Comprendre les deepfakes »** – Vidéo de 3 minutes expliquant ce que sont les deepfakes générés par l'IA, comment les reconnaître et comment s'en protéger
- **« Les escroqueries conversationnelles à la loupe »** – Vidéo de 3 minutes expliquant ce que sont les escroqueries conversationnelles générées par l'IA, comment les reconnaître et comment s'en protéger

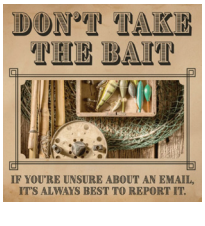
Images

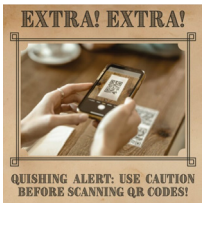
Nous avons également créé des images à ajouter aux emails, aux canaux de chat, aux réunions virtuelles et aux autres communications pour renforcer le thème « Détective en cybersécurité ».

- Infographie **« Signalement des emails suspects »** – Utilisez cette infographie sur le thème du détective pour fournir des informations détaillées sur les messages malveillants.
- GIF animé **« Détective en cybersécurité »** – Partagez ces animations sur le thème du détective sur vos canaux numériques.
- Quatre images **« Sensibilisation à la cybersécurité »** – Utilisez ces images sur le thème du détective pour renforcer les sujets de formation.
- Cinq arrière-plans virtuels **« Détective en cybersécurité »** – Mettez en avant le thème du détective pendant les réunions virtuelles et les vidéoconférences.

Tous les contenus sont disponibles dans 13 langues :

- Anglais (États-Unis)
- Arabe (Égypte)
- Français (Canada)
- Français (France)
- Allemand (Allemagne)
- Italien (Italie)
- Japonais (Japon)
- Coréen (Corée)
- Portugais (Brésil)
- Espagnol (Espagne)
- Espagnol (Amérique latine)
- Chinois simplifié
- Chinois traditionnel





Vous aurez accès aux fichiers de conception et aux fichiers image pour tous les graphismes. Vous aurez la possibilité de modifier ces éléments pour refléter la culture de votre entreprise et renforcer l'engagement à l'égard du programme. Vous pourrez par exemple :

- Redimensionner les ressources selon différentes tailles d'impression et d'affichage
- Ajouter le logo et les éléments de marque de votre entreprise
- Modifier le texte et les couleurs

Un mois avant le lancement

Planifiez votre campagne

Pendant la préparation du lancement de votre campagne, assurez-vous d'être prêt à annoncer la nouvelle.

- **Parcourez nos suggestions de ressources et de communications** pour déterminer ce que vous utiliserez ou non pendant votre campagne.
- **Modifiez les fichiers graphiques** si nécessaire.
- **Identifiez vos méthodes de distribution** des contenus et des communications (p. ex., email, canaux de chat internes, portail partagé et/ou wiki interne).
- **Partagez votre plan** avec les principales parties prenantes et les décideurs clés, puis corrigez-le si nécessaire. Utilisez l'un de nos arrière-plans virtuels « Détective en cybersécurité » si la discussion a lieu par vidéoconférence.
- **Obtenez l'adhésion** de la direction et des équipes transversales pour amplifier l'impact de votre campagne.
- **Déterminez la date de lancement**, la date de fin, et les principales dates intermédiaires.

Créez un référentiel de contenus centralisé

Nous vous recommandons d'utiliser un référentiel centralisé (comme un wiki interne), où vous réunirez toutes les ressources de formation destinées aux utilisateurs de la campagne. Vous n'aurez ainsi plus besoin d'envoyer tous vos contenus par email ou via des canaux de chat, et les collaborateurs pourront gérer la plupart des activités qui leur sont attribuées à partir d'une même interface.

Créez un canal de chat interne

Si ce n'est pas déjà fait, créez un canal de chat interne dédié à la formation et à la sensibilisation à la cybersécurité. Il s'agit d'un moyen simple et rapide d'envoyer des rappels concernant les activités du programme et les dates importantes.

La semaine avant le lancement

Annoncez la campagne à venir

La semaine précédant le lancement officiel de votre campagne, nous vous recommandons d'envoyer à l'ensemble des collaborateurs un email offrant un aperçu du programme à venir. 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.

- Partagez le GIF animé « Détective en cybersécurité » ainsi que cette suggestion de communication par email ou via le canal de chat interne (à modifier si nécessaire) :

OBJET :
Disponible prochainement : campagne « Détective en cybersécurité »

Le <date>, nous lancerons une nouvelle campagne de sensibilisation à la cybersécurité intitulée « Détective en cybersécurité ». Pendant un mois, vous aurez accès à des informations et à des ressources de formation qui expliquent l'importance de signaler les messages suspects, qui représentent un risque majeur pour les entreprises et les personnes du monde entier.

Chacun d'entre nous a un rôle à jouer dans la défense contre les emails de phishing et autres cyberattaques. Ce programme vous fournira des ressources et des conseils précieux pour renforcer votre protection chez vous et au travail.

Restez connectés ! *<insérer les détails de la réunion virtuelle>*

SEMAINE 1

Ça vient de sortir ! Signalez les emails suspects.

Lancez votre programme

- Organisez une session de lancement et utilisez un arrière-plan virtuel pour présenter le thème.
- Expliquez aux participants qu'ils recevront des emails hebdomadaires contenant des liens vers les ressources de la campagne.
- Dans votre référentiel de contenus, ajoutez le module vidéo « Détective en cybersécurité : signalement des emails suspects » et l'image « Ne tombez pas dans le piège ».
- Envoyez un message par email ou via le canal de chat interne en utilisant cette suggestion de texte (à modifier si nécessaire) :

  OBJET :
  Ça vient de sortir ! Signalez les emails suspects

  Les dispositifs techniques de protection ne peuvent pas toujours nous sauver la mise. Il est donc important que nous prenions conscience de notre rôle dans la sécurité de notre entreprise. Cette vidéo de deux minutes sur le signalement des emails suspects présente les principes de base des emails de phishing, et explique comment les reconnaître et s'en protéger. Ne tombez pas dans le piège.

  Cliquez sur le lien suivant pour regarder la vidéo au moment qui vous convient. Il est essentiel de la visionner pour tirer le meilleur parti des autres supports que nous partagerons cette semaine. *<[insérer le lien]>*

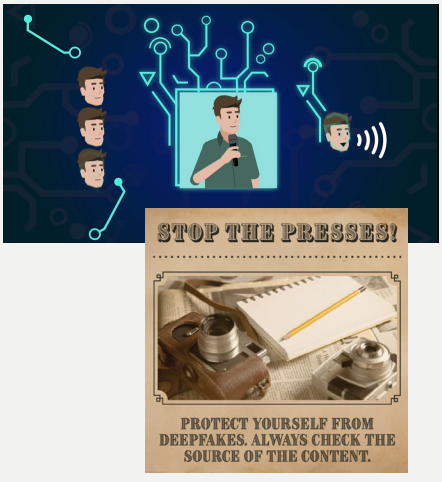
- Plus tard dans la semaine, partagez l'image à titre de rappel.
  Voici une suggestion de message :

  Ne tombez pas dans le piège. Vous êtes la dernière ligne de défense de notre entreprise contre les emails de phishing. N'oubliez pas de signaler systématiquement les emails suspects.

SEMAINE 2

Info de dernière minute ! Soyez à l'affût de l'IA (Partie 1)

Encouragez la participation



- Au début de la semaine 2, ajoutez le module vidéo « Comprendre les deepfakes » et l'image « Info de dernière minute ! ».
- Envoyez un message de rappel par email ou via les canaux de chat internes en utilisant le texte suivant (à modifier si nécessaire).

  OBJET :
  Info de dernière minute ! Soyez à l'affût de l'IA (Partie 1)

  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 aujourd'hui.)

  Aujourd'hui, nous allons regarder une autre vidéo, qui explique cette fois comment l'IA générative complique la détection du phishing. En trois minutes, elle vous aidera à comprendre les deepfakes et vous montrera une nouvelle technique utilisée par les cybercriminels pour tenter de vous piéger. *<[insérer le lien]>*

- Plus tard dans la semaine, partagez l'image à titre de rappel.
  Voici une suggestion de message :

  Info de dernière minute ! Protégez-vous contre les deepfakes. Ce type de phishing généré par l'IA peut imiter des figures d'autorité dans des vidéos, des images ou des extraits vocaux pour diffuser des informations délibérément fausses.

SEMAINE 3

Alerte ! Ne ratez pas notre numéro exclusif !

Saluez les efforts de participation

- Au début de la semaine 3, ajoutez l'infographie « Signalement des emails suspects » et l'image « Alerte au quishing ! ».
- Envoyez un message de rappel par email ou via les canaux de chat internes en utilisant le texte suivant (à modifier si nécessaire).

  OBJET :
  Alerte ! Ne ratez pas notre numéro exclusif !

  Félicitations à tous ceux qui se sont glissé dans la peau d'un détective en cybersécurité et qui ont tiré parti de nos supports dédiés.

  Nous avons ajouté une nouvelle ressource à *<[insérer le lien]>* : l'infographie « Signalement des emails suspects ». Elle vous aidera à représenter visuellement l'identification et le signalement des emails suspects en toute sécurité. Les cybercriminels cherchent en permanence de nouveaux moyens de nous piéger, par exemple avec le phishing par code QR ou « quishing ».

- Plus tard dans la semaine, partagez l'image à titre de rappel.
  Voici une suggestion de message :

  Alerte au quishing ! Évitez de scanner des codes QR non sollicités provenant de sources inconnues ou inattendues, qu'ils soient physiques ou électroniques.

SEMAINE 4

Identifiez, puis signalez ! Soyez à l'affût de l'IA (Partie 2)

Envoyez une invitation à la réunion de clôture

- Au début de la dernière semaine, ajoutez le module vidéo « Les escroqueries conversationnelles à la loupe » et l'image « Si vous identifiez une menace, signalez-la ».
- Envoyez un message pour rappeler aux collaborateurs de terminer toutes les activités, ainsi qu'une invitation à participer à une réunion virtuelle de clôture.

  OBJET :
  Identifiez, puis signalez ! Soyez à l'affût de l'IA (Partie 2).

  Nous espérons que les ressources « Détective en cybersécurité » que nous avons partagées avec vous ces dernières semaines vous ont été utiles.
  Pour conclure, nous avons ajouté une dernière vidéo « Les escroqueries conversationnelles à la loupe » ici : *<[insérer le lien]>*. Cette vidéo de trois minutes s'attarde sur un nouveau type de phishing généré par l'IA.

  Et n'oubliez pas ce que dit cette image *<[insérer le lien]>* : « Si vous identifiez une menace, signalez-la ». Assurez-vous de signaler les incidents de sécurité sans tarder ! En intervenant rapidement, il est possible d'éviter une compromission.

  Vous êtes également invité à une réunion virtuelle de clôture, où nous discuterons de témoignages en lien avec cette campagne, rendrons hommage à nos participants et solliciterons vos commentaires. *<insérer les détails de la réunion>*

  Pour toute question ou tout commentaire, n'hésitez pas à me contacter à l'adresse *<[email]>*.

Clôture de votre campagne

Organisez une réunion de clôture

Le moment est venu de clôturer la campagne « Détective en cybersécurité ». Utilisez l'un des arrière-plans virtuels pendant la réunion de clôture. Si possible, ouvrez la discussion sur des points importants, tels que les suivants :

- Les points positifs et négatifs de la campagne, d'après les participants
- Les enseignements qu'ils en ont tirés
- Les points à approfondir

Pour encore plus d'impact…

Devenez client Proofpoint

Ce kit du mois de sensibilisation à la cybersécurité s'inscrit dans le cadre d'une campagne plus vaste, intitulée « Détective en cybersécurité », exclusivement accessible aux clients Proofpoint. Cette campagne s'appuie sur le contenu de ce document, vous offrant un mois complet d'outils de communication et de contenus de sensibilisation qui encouragent une participation active.

Les clients Proofpoint ont accès à un large éventail de ressources essentielles :

- **Un guide de campagne**, qui va plus loin que ce document avec des contenus et informations supplémentaires
- **Des modules supplémentaires**, qui s'intéressent de près aux bonnes pratiques en matière de navigation Web
- **Des cartes postales** pour informer les utilisateurs de la campagne à venir et encourager la participation
- **Des fiches de suivi des activités** pour aider les utilisateurs à consigner les activités qu'ils ont terminées
- **Des badges** à envoyer aux utilisateurs lorsqu'ils terminent leurs activités hebdomadaires
- **Des incentives**, comme des autocollants à imprimer, qui récompensent la participation
- **Des contenus à partager**, comme des affiches, des économiseurs d'écran animés, des images de sensibilisation et une newsletter pour partager des conseils et des rappels tout au long de la campagne

Contactez-nous pour bénéficier d'une démonstration.

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.