Proofpoint Security Awareness Training – Contenu

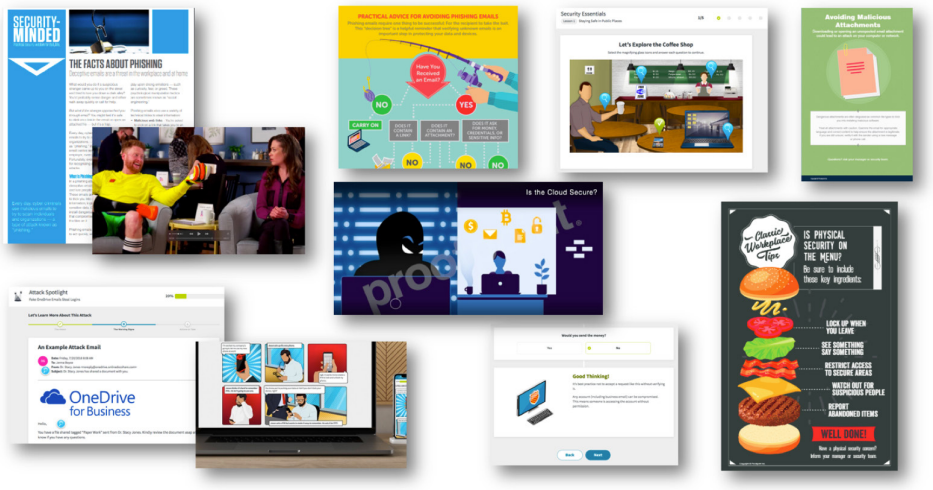
Comment former vos collaborateurs à reconnaître et à éviter les risques

PRINCIPAUX AVANTAGES

Réduction des risques liés aux utilisateurs

- Évaluer les vulnérabilités des utilisateurs grâce à des simulations d'attaques permettant d'identifier les types de risques
- Fournir une formation immédiate pour prévenir les attaques futures
- Éprouver les connaissances en sécurité des utilisateurs
- Stimuler un changement positif grâce à des modules de formation faciles à consulter
- Offrir une formation localisée, selon l'emplacement géographique des utilisateurs, partout dans le monde
- Sensibiliser les utilisateurs aux problématiques de sécurité grâce à des supports et communications personnalisables

Le programme Proofpoint Security Awareness Training propose des formations reposant sur des principes pédagogiques à l'efficacité reconnue, qui renforcent l'efficacité de l'apprentissage. Nos simulations d'attaques ThreatSim® et nos évaluations des connaissances CyberStrength® vous permettent de mieux comprendre les risques liés à vos collaborateurs. Tous secteurs confondus, les clients Proofpoint témoignent de l'efficacité de nos divers modules de formation. Ceux-ci vous aident à proposer la formation appropriée aux personnes concernées afin de favoriser les bons comportements. Cette approche permet en fin de compte de réduire les risques liés aux utilisateurs. De plus, nos supports de sensibilisation à la sécurité renforcent le contenu des modules.



Le programme Proofpoint Security Awareness Training propose un large éventail de formations et d'autres ressources.

Évaluations

Comprendre les vulnérabilités particulières de vos collaborateurs est essentiel pour pouvoir leur proposer des formations de sensibilisation à la sécurité personnalisées, et identifier plus globalement les risques de cybersécurité pour votre entreprise. Nos simulations d'attaques ThreatSim vous aident à évaluer la vulnérabilité de vos utilisateurs face aux menaces réelles. Elles mettent en scène différents types de menaces, notamment des attaques de phishing ou des clés USB au contenu malveillant. Quant aux évaluations CyberStrength, elles vous aident à déterminer le niveau de connaissances de vos collaborateurs en ce qui concerne divers aspects de la cybersécurité.

SIMULATIONS D'ATTAQUES THREATSIM – PHISHING ET CLÉS USB

Modèles de simulations d'attaques

Divers types d'attaques sont mis en scène, notamment des pièces jointes malveillantes, des liens intégrés, des clés USB au contenu malveillant et des demandes de données personnelles. Vous avez le choix parmi des milliers de modèles dans plus de 36 langues.

Catégories de modèles :

- Cloud
- Commercial
- Particulier
- Entreprise
- Threat intelligence Proofpoint
- Saisonnier
- USB
- Sectoriel

Pages de renvoi proposant des messages « éducatifs »

Utilisez des messages de formation ponctuels qui s'affichent lorsqu'un collaborateur interagit avec un faux email de phishing. Ces pages de renvoi proposent des informations sur la menace et expliquent ses conséquences potentielles en cas de véritable attaque. De plus, elles prodiguent des conseils afin d'éviter de futures attaques.

Types de messages « éducatifs » :

- Personnalisé
- Intégré
- Messages d'erreur
- Interactif
- Vidéo

ÉVALUATIONS DES CONNAISSANCES CYBERSTRENGTH

Évaluations des connaissances personnalisées et prédéfinies

Évaluez les connaissances des utilisateurs sur divers sujets liés à la sécurité, au-delà des simulations d'attaques. Vous avez le choix parmi plus de 400 questions prédéfinies et vous pouvez y ajouter les vôtres. Il existe 17 évaluations des connaissances prédéfinies dans de nombreuses catégories.

Évaluations des connaissances prédéfinies :

- Évaluation globale, 55 questions
- Évaluation globale, 33 questions
- Évaluation globale, 22 questions
- RGPD
- Menaces internes
- Sécurité en ligne
- Protection des mots de passe
- PCI (Payment Card Industry)
- Phishing
- Données personnelles
- Prévention des compromissions
- Protection des informations médicales
- Protection des données personnelles
- Protection de la messagerie électronique – Notions avancées
- Protection de la messagerie électronique – Notions fondamentales
- Mesures de sécurité
- Sécurité mobile

Modules de formation Proofpoint

Nos modules de formation primés sont personnalisables et se déclinent sous forme de jeux, de vidéos et de contenus interactifs. Ils s'inspirent de principes pédagogiques destinés à stimuler des changements de comportement. Pour rester pertinents malgré un paysage des menaces en constante évolution, ils s'appuient sur les informations de threat intelligence collectées par Proofpoint.

À propos des modules

- Les leçons sont courtes et se concentrent sur un seul sujet. En moyenne, il ne faut que 5 à 15 minutes pour suivre un module complet. Cette approche permet de capter et conserver l'attention des utilisateurs tout au long de la formation. Ils seront ainsi plus susceptibles d'en mémoriser le contenu.
- Le contenu est personnalisable, pour garantir son adéquation aux besoins de vos utilisateurs. Notre Customization Center en libre-service vous permet de modifier le texte, les écrans, les images, les questions et les réponses, et même de réorganiser le contenu.
- Il est possible d'inscrire automatiquement des utilisateurs à un module particulier à la suite d'une évaluation, pour garantir qu'ils reçoivent la formation appropriée au moment opportun.
- Les modules de formation sont conçus pour être consultables sur des terminaux mobiles. Les utilisateurs peuvent ainsi suivre les formations à tout moment, n'importe où, sur tout terminal connecté.
- Les modules interactifs Proofpoint sont conformes aux exigences de la section 508 et aux directives WCAG 2.0 AA (directives d'accessibilité des contenus Web).

- Les collaborateurs peuvent tirer parti de nos formations partout dans le monde. Nos modules sont traduits dans plus de 35 langues et peuvent être adaptés à la région où réside l'utilisateur. Le contenu est traduit par des traducteurs professionnels et adapté à l'aide de références régionales.

Modules de formation

- Avoiding Dangerous Attachments (Identification des pièces jointes dangereuses)
- Vidéo : Avoiding Dangerous Attachments (Identification des pièces jointes dangereuses)
- Avoiding Dangerous Links (Identification des liens dangereux)
- Vidéo : Avoiding Dangerous Links (Identification des liens dangereux)
- Beyond Passwords (Au-delà des mots de passe)
- Business Email Compromise (Lutte contre le piratage de la messagerie en entreprise)
- Vidéo : Business Email Compromise (Lutte contre le piratage de la messagerie en entreprise)
- Vidéo de sensibilisation : Confidential Information (Informations confidentielles)
- Attack Spotlight : COVID-19 (Coronavirus) Phishing Scams (Arnaques de phishing exploitant le COVID-19 (coronavirus))
- Data Entry Phishing (Phishing et saisie de données)
- Vidéo : Data Entry Phishing (Phishing et saisie de données)
- Data Protection and Destruction (Protection et destruction des données)
- Attack Spotlight : DocuSign Phishing Campaign (Campagne de phishing DocuSign)
- Vidéo de sensibilisation : Don't Be a Jan (Les comportements à éviter)
- Email Protection Tools (Outils de protection de la messagerie électronique)
- Email Security (Sécurité de la messagerie)
- Email Security on Mobile Devices (Sécurité de la messagerie sur les terminaux mobiles)
- Attack Spotlight : Fake OneDrive Emails Steal Logins (Faux emails OneDrive utilisés dans le vol d'identifiants)
- FERPA For Higher Education (Family Educational Rights and Privacy Act pour l'enseignement supérieur)
- Attack Spotlight : Fraudulent Shipping Notifications (Avis de livraison frauduleux)
- GDPR in Action (Le RGPD en action)
- GDPR Overview (Présentation du RGPD)
- Healthcare Data Protection (Protection des données dans le secteur de la santé)
- Healthcare Privacy Data Overview (Présentation de la confidentialité des données dans le secteur de la santé)
- Healthcare Privacy Violation (Violation de la confidentialité des données dans le secteur de la santé)
- Vidéo de sensibilisation : How to Report a Phish (Signaler un email de phishing)
- Insider Threat Overview (Présentation des menaces internes)
- Vidéo : Insider Threat Overview (Présentation des menaces internes)
- Introduction to Phishing (Introduction au phishing)
- Vidéo : Introduction to Phishing (Introduction au phishing)
- Vidéo de sensibilisation : Is the Cloud Secure? (Le cloud est-il sécurisé ?)
- Vidéo de sensibilisation : Lock Before You Walk – Dr. (Verrouillez votre poste de travail – Soins de santé)
- Vidéo de sensibilisation : Lock Before You Walk – Human Resources (Verrouillez votre poste de travail – Ressources humaines)
- Malicious Insider Threat (Menaces internes liées à des personnes malintentionnées)
- Mitigating Compromised Devices (Réduire les risques liés aux terminaux compromis)
- Mobile App Permissions (Autorisations pour les applications mobiles)
- Mobile App Security (Sécurité des applications mobiles)
- Mobile Device Security (Sécurité des terminaux mobiles)
- Vidéo : Mobile Device Security (Sécurité des terminaux mobiles)
- Multi-Factor Authentication - MFA (Authentification multifacteur)
- OWASP Fundamentals (OWASP – Notions fondamentales)
- Password Management (Gestion des mots de passe)
- Password Policy (Règles en matière de mots de passe)
- PCI DSS
- Physical Security (Sécurité physique)
- Vidéo : Physical Security (Sécurité physique)
- PII Fundamentals (Données personnelles – Notions fondamentales)
- Vidéo : PII Fundamentals (Données personnelles – Notions fondamentales)
- PII in Action (Données personnelles en action)
- Vidéo : PIN and Password Protection (Protection des codes PIN et des mots de passe)
- Protected Health Information – PHI (Protection des informations médicales)
- Protecting Against Ransomware (Protection contre les ransomwares)
- Safe Social Networking (Sécurité sur les réseaux sociaux)
- Vidéo : Safe Social Networking (Sécurité sur les réseaux sociaux)
- Safer Web Browsing (Navigation plus sécurisée)
- Security Beyond the Office (Sécurité à l'extérieur du bureau)
- Security Essentials (Principes fondamentaux de la sécurité)
- Vidéo : Security Essentials (Principes fondamentaux de la sécurité)
- Security Essentials – Executive (Principes fondamentaux de la sécurité pour les dirigeants)
- Social Engineering (Ingénierie sociale)
- Spear-Phishing Threats (Attaques de spear phishing)
- Vidéo de sensibilisation : Think Before You Click – Great Saves (Réfléchissez avant de cliquer – Un excellent gardien)
- Vidéo de sensibilisation : Think Before You Click (Réfléchissez avant de cliquer)
- Vidéo de sensibilisation : Think Before You Post – Social Media (Réfléchissez avant de partager – Réseaux sociaux)
- Travel Security (Sécurité lors des déplacements)

- Vidéo : Travel Security (Sécurité lors des déplacements)
- Unintentional Insider Threat (Menaces internes accidentelles)
- URL Training (Formation en matière d'URL)
- USB Device Safety (Sécurité des périphériques USB)
- Vidéo de sensibilisation : Use Caution on Public Wi-Fi (Utilisez le Wi-Fi public avec prudence)
- Vidéo de sensibilisation : What is Email Fraud? (Qu'est-ce que la fraude par email ?)
- Vidéo de sensibilisation : Why Your Security Awareness Training Program is Important (Pourquoi se former à la sécurité ?)
- Workplace Security in Action (La sécurité sur le lieu de travail en action)

Modules de formation de nos partenaires

Nous collaborons avec divers éditeurs réputés pour étoffer notre gamme de contenus et de types de formations. Tous ces contenus sont validés par nos équipes pédagogiques et de développement pour garantir la continuité et la cohérence de l'apprentissage.

- Proofpoint a racheté The Defence Works en mai 2020. Cet éditeur propose une grande variété de contenus présentés sous forme divertissante et humoristique, qui aident à capter l'attention des utilisateurs par leur approche novatrice.
- TeachPrivacy est spécialisé dans les réglementations et obligations liées à la confidentialité. Grâce à ses contenus riches et complets, vous pouvez adapter votre formation en matière de conformité et de confidentialité à votre culture d'entreprise et à vos problématiques particulières.

Contenus The Defence Works

- Vidéo The Defence Works : A Sneaking Suspicion (Méfiance !)
- Vidéo The Defence Works : A Step Too Far (Cela va trop loin)
- Vidéo The Defence Works : Agent Smith
- Vidéo The Defence Works : An Unexpected Call (Un appel inattendu)
- The Defence Works : Anti-Fraud and Bribery (Lutte contre la fraude et les pots-de-vin)
- The Defence Works : Anti-Money Laundering (Lutte contre le blanchiment)
- Vidéo The Defence Works : Backup Bob
- The Defence Works : BEC Scams (Piratage de la messagerie en entreprise)
- Vidéo The Defence Works : Behind Closed Doors (À huis clos)
- Vidéo The Defence Works : Behind Your Back (Dans votre dos)
- Vidéo The Defence Works : Cooking with a Con! (Cuisine et petites arnaques)
- Vidéo The Defence Works : Deadline Demands (Dates limites)
- Vidéo The Defence Works : Don't Bet on It (Ne pariez pas là-dessus)
- Vidéo The Defence Works : Don't Click on That! (Ne cliquez pas !)
- Vidéo The Defence Works : Double « Oh… No » (Grave erreur !)
- Vidéo The Defence Works : Fake It 'Til You Make It (Faites semblant)
- The Defence Works : Freedom of Information (Liberté d'information)
- The Defence Works : GDPR Awareness (Global) (Sensibilisation au RGPD – Monde)
- The Defence Works : GDPR Awareness (UK) (Sensibilisation au RGPD – Royaume-Uni)
- The Defence Works : Incident Reporting (Signalement d'incidents)
- The Defence Works : Menaces internes
- Vidéo The Defence Works : Internet-Enabled Nightmare (Cauchemar sur Internet)
- The Defence Works : Introduction to Phishing Emails and Websites (Introduction aux emails et sites de phishing)
- The Defence Works : Malware & Ransomware (Malwares et ransomwares)
- The Defence Works : Mobile Device Defence (Protection des terminaux mobiles)
- The Defence Works : Modern Slavery (Esclavagisme moderne)
- Vidéo The Defence Works : Nerves of Steel (Des nerfs d'acier)
- Vidéo The Defence Works : Oh… My Password! (Ciel, mon mot de passe !)
- The Defence Works : PCI DSS
- The Defence Works : Perfect Your Password (Optimiser votre mot de passe)
- The Defence Works : Personally Identifiable Information (Données personnelles)
- Vidéo The Defence Works : Phishing Emails in Real Life (Emails de phishing dans la vie réelle)
- The Defence Works : Physical Security (Sécurité physique)
- Vidéo The Defence Works : Prison Break… In? (Par effraction)
- The Defence Works : Privileged Access Awareness (Sensibilisation aux accès avec privilèges)
- The Defence Works : Protecting Data (Protection des données)
- The Defence Works : Secure Printing (Impression sécurisée)
- The Defence Works : Security Beyond the Office (Sécurité à l'extérieur du bureau)
- The Defence Works : Shielding Against Spear Phishing (Protection contre le spear-phishing)
- Vidéo The Defence Works : Sleepy Security (Sécurité en dormance)
- Vidéo The Defence Works : So Much Data! (Tant de données !)
- The Defence Works : Social Engineering (Ingénierie sociale)
- Vidéo The Defence Works : Social Media Roller Coaster (Les montagnes russes des réseaux sociaux)
- The Defence Works : Social Networking (Réseaux sociaux)
- The Defence Works : Spotting Invoice Scams (Repérer les arnaques aux factures)
- The Defence Works : Surfing the World Wide Web (Navigation Web)
- Vidéo The Defence Works : Swiped Right Into Trouble (Faites glisser à droite... et à vous les ennuis)
- Vidéo The Defence Works : TAKEOVER: BEC Scams (Piratage de comptes : arnaques BEC)
- Vidéo The Defence Works : TAKEOVER: Digging for Data (Piratage de comptes : à la recherche de données)
- The Defence Works : The Hazards of Hacking (Les risques du piratage)
- Vidéo The Defence Works : Under Surveillance (Sous surveillance)

- Vidéo The Defence Works : What Is It, My Child? (Oui, mon enfant ?)
- The Defence Works : Working From Home (Télétravail)
- The Defence Works : Working From Home – COVID-19 (Télétravail – COVID-19)
- The Defence Works : You, Me & Data Protection – GDPR Recap (Vous, moi et la protection des données – Résumé du RGPD)

Contenus TeachPrivacy

- Vidéo TeachPrivacy : California Health Privacy (Obligations de confidentialité dans le secteur de la santé en Californie)
- TeachPrivacy : CCPA (California Consumer Privacy Act – Loi californienne sur la confidentialité des données des particuliers)
- TeachPrivacy : CCPA – Interactive Whiteboard (CCPA – Tableau interactif)
- Vidéo TeachPrivacy : FERPA – For Higher Education (Family Educational Rights and Privacy Act pour l'enseignement supérieur)
- TeachPrivacy : FERPA – K-12 (Family Educational Rights and Privacy Act pour l'enseignement primaire et secondaire)
- TeachPrivacy : FERPA – Interactive Whiteboard (Family Educational Rights and Privacy Act – Tableau interactif)
- TeachPrivacy : FTC Red Flags (Indicateurs d'alerte de la Federal Trade Commission)
- Vidéo TeachPrivacy : GDPR (RGPD)
- TeachPrivacy : GDPR – Interactive Whiteboard (RGPD – Tableau interactif)
- TeachPrivacy : GLBA (Gramm-Leach-Bliley Act – Loi sur les transactions financières aux États-Unis)
- TeachPrivacy : Global Privacy and Data Protection (Protection de la confidentialité et des données à l'international)
- TeachPrivacy : HIPAA – Interactive Whiteboard (Health Insurance Portability and Accountability Act – Tableau interactif)
- Vidéo TeachPrivacy : HIPAA Overview (Présentation de la loi HIPAA)
- Vidéo TeachPrivacy : HIPAA Privacy for Covered Entities (Confidentialité HIPAA pour les entités concernées)
- Vidéo TeachPrivacy : Malware
- Vidéo TeachPrivacy : PCI
- TeachPrivacy : Privacy Training for Federal Government Contractors (Formation sur la confidentialité à l'intention des sous-traitants du gouvernement fédéral)
- TeachPrivacy : Secure Workplace: Game (Un lieu de travail sûr : Jeu)
- TeachPrivacy : Texas Health Privacy (Obligations de confidentialité dans le secteur de la santé au Texas)
- TeachPrivacy : The Ransomware Attack (Attaque de ransomware)

Supports de sensibilisation à la sécurité

Pour soutenir vos projets de formation et de sensibilisation, nous proposons un large éventail de modules, vidéos, affiches, images, newsletters, articles, infographies, etc. Ces supports sont destinés à favoriser les discussions sur la cybersécurité avec vos collaborateurs. En faisant de la sécurité une priorité bien présente à l'esprit de vos collaborateurs, vous pouvez contribuer à réduire le niveau de risque pour votre entreprise.

- Vous pouvez personnaliser la plupart des supports de sensibilisation en y ajoutant le logo de votre entreprise. Vous pouvez accéder aux fichiers d'origine sur le portail Supports de sensibilisation à la sécurité.
- De nombreux supports de sensibilisation sont disponibles en 20 langues.

Attack Spotlight : Informez vos utilisateurs sur les menaces en activité. Ce contenu en phase avec l'actualité des menaces s'inspire d'attaques de phishing, de leurres et de techniques observés sur le terrain par la threat intelligence de Proofpoint.

- COVID-19 (Coronavirus)
- DocuSign Phishing (Messages de phishing DocuSign)
- Domain Fraud (Fraudes liées aux domaines)
- Fake Browser Updates (Fausses mises à jour de navigateur)
- Fraudulent Shipping Notifications (Avis de livraison frauduleux)
- Look-Alike Websites Trick Users (Sites Web falsifiés pour tromper les utilisateurs)
- Microsoft 365 (Office 365) Credential Phishing (Phishing d'identifiants de connexion pour Microsoft 365 (Office 365))
- OneDrive Phishing Campaign (Campagne de phishing OneDrive)
- Phishing Campaign Delivers Dangerous Trojan (Une campagne de phishing injecte un cheval de Troie dangereux)
- Scammers Mimic Real Banking Emails (Des cyberescrocs imitent de vrais emails des banques)

Alertes sur les menaces : Avertissez rapidement vos utilisateurs de l'existence d'attaques spécifiques détectées par la threat intelligence de Proofpoint.

- COVID-19 Credential Phishing – U.S. Retailers (Phishing d'identifiants exploitant le COVID-19 – Détaillants USA)
- COVID-19 Phish Spreading Malware – U.S. Infrastructure (Phishing exploitant le COVID-19 pour propager des malwares – Infrastructures USA)
- WebEx Credential Phishing Lures (Leurres de phishing d'identifiants ciblant WebEx)
- Zoom Credential Phishing Lures (Leurres de phishing d'identifiants ciblant Zoom)
- Zoom Phishing Attacks Spread Malware (Attaques de phishing ciblant Zoom pour propager des malwares)
- Et plus encore chaque semaine

Vidéos de sensibilisation : Sensibilisez vos collaborateurs à l'importance de la sécurité grâce à ces vidéos.

- Série Un excellent gardien
- Série Barrez la porte aux voleurs
- Série Les comportements à éviter
- Série Le cloud est-il sûr ?
- What Are BEC Attacks? (Qu'est-ce qu'une attaque BEC ?)
- Qu'est-ce que la fraude par email ?
- What Is Phishing? (Qu'est-ce que le phishing ?)
- What Is Ransomware? (Qu'est-ce qu'un ransomware ?)
- What Is Smishing? (Qu'est-ce que le SMiShing ?)
- What Is the IoT? (Qu'est-ce que l'IoT ?)
- What Is Vishing? (Qu'est-ce que le vishing ?)
- Pourquoi se former à la sécurité ?

Infographies

- Piratage de la messagerie en entreprise
- Internet of Things (Internet des objets)
- Phishing Decision Tree (Arbre de décision du phishing)
- Phishing: A Scammer's Sinister Scheme (Phishing : le mauvais plan d'un cyberescroc) – version normale et version longue
- Tax-Related Schemes (Escroqueries liées aux impôts)
- Comprendre les ransomwares
- Etc.

Newsletters et articles

- Newsletters et articles sur divers sujets : rentrée scolaire, pièces jointes et liens malveillants, achats pour les fêtes de fin d'année, menaces internes, mots de passe, phishing, sécurité physique, conseils lors des déplacements, etc.

Affiches

- Identification des pièces jointes malveillantes
- Be Smart About Mobile Security (Optimisez la sécurité de vos terminaux mobiles)
- Destination inconnue – Sécurité des URL
- Dangerous USB Devices (Périphériques USB dangereux)
- Is Physical Security on the Menu? (La sécurité physique est-elle au menu ?)
- Not All Offers Are as Sweet as They Seem (Toutes les offres ne sont pas aussi alléchantes qu'elles en ont l'air)
- Etc.

Divers

- Graphismes et instructions pour créer du contenu supplémentaire
- Jeu « Cybersecurity Consequences » (Cybersécurité et conséquences)
- Post-it « Lock Before You Walk » (Verrouillez votre poste de travail)
- Mimes
- Cartes postales
- Jeux de mots cachés
- Etc.

Documentation liée au programme

Pour garantir la réussite d'un programme, tous les intervenants doivent comprendre les raisons de leur participation et ce que l'on attend d'eux. Voilà pourquoi nos programmes de sensibilisation à la sécurité incluent des conseils d'experts afin de guider les administrateurs pour leur mise en œuvre. Nous proposons également des communications ciblées destinées aux utilisateurs et aux principales parties prenantes. Notre documentation est organisée en quatre catégories :

- Bonnes pratiques
- Clés de la réussite
- Campagnes
- Présentations

Ces informations aideront les administrateurs des programmes de formation à établir une relation de confiance avec les utilisateurs et à instaurer une culture de sensibilisation à la sécurité.

Bonnes pratiques : Notre documentation sur les bonnes pratiques aide les administrateurs à choisir les stratégies les plus efficaces pour amener des changements de comportement. Elle vous sera utile, que votre programme en soit à ses débuts ou qu'il soit en place depuis longtemps. Elle inclut des informations sur les calendriers d'activités, des bonnes pratiques et divers plans de mise en œuvre d'un programme.

Campagnes : Les campagnes simplifient l'administration et vous aident à créer des expériences utilisateur optimales. Elles comprennent tous les contenus ressources de communication interne nécessaires pour déployer un projet de sensibilisation à la sécurité multicanal au sein de votre entreprise.

Clés de la réussite : Ces podcasts, webinaires, études et autres contenus sont destinés à vos administrateurs. Ils ont pour but de les aider à expliquer l'intérêt des formations de sensibilisation à la sécurité à leurs publics cibles, à stimuler la participation à des formations supplémentaires, à guider les débats sur la modélisation des conséquences, etc.

Présentations : Ces présentations scriptées et préenregistrées couvrent un large éventail de sujets tels que le phishing, l'usurpation d'identité et le signalement des emails suspects. Les administrateurs peuvent les utiliser pour des formations individualisées ou des sessions en ligne.

EN SAVOIR PLUS

Essayez des versions de démonstration de nos modules de formation et consultez nos contenus de sensibilisation à la sécurité sur la page **https://www.proofpoint.com/fr/resources/try-security-awareness-training**.