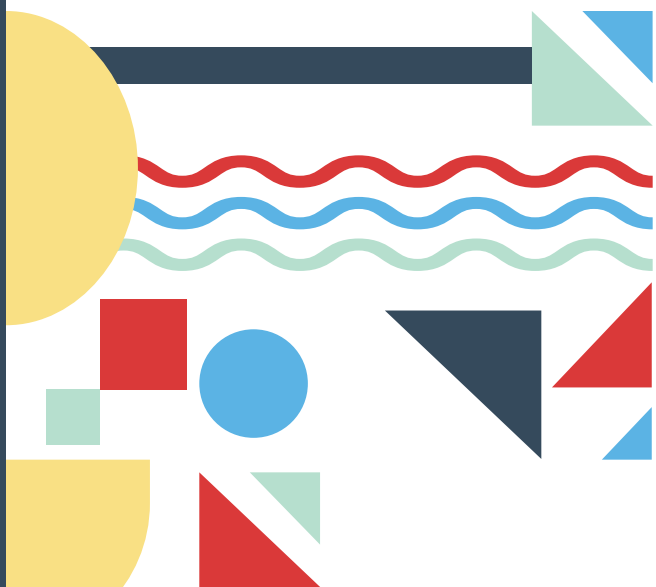
FORTRA

Guide ultime de la formation en sensibilisation à la sécurité :

Les 4 piliers d’une formation en sensibilisation à la sécurité réussie

TABLE DES MATIÈRES



Qu’est-ce que la sensibilisation à la sécurité ?

Une formation en sensibilisation à la sécurité est un programme d’apprentissage en ligne. Elle enseigne aux utilisateurs d’une organisation comment protéger les informations confidentielles contre les cybercriminels. Dans ce contexte, le terme « utilisateurs » peut comprendre des employés à temps plein et à temps partiel, des pigistes et toute autre personne pouvant accéder, partager, stocker ou modifier des données organisationnelles.

Les cours des formations en sensibilisation à la sécurité, ainsi que les sujets abordés, doivent répondre aux objectifs globaux de l’organisation en matière de cybersécurité et permettre de modifier les comportements des utilisateurs qui posent des risques. Parmi ces comportements, notons le fait de cliquer sur un lien, de réutiliser des mots de passe ou de saisir des informations sensibles dans un formulaire sur une page Web suspecte.

Les meilleurs programmes de formation en sensibilisation à la sécurité utilisent des simulations d’hameçonnage basées sur des exemples réels et d’autres outils de communication et de renforcement. L’objectif principal de ces campagnes est de réduire les coûts associés à d’éventuelles brèches de sécurité et de mitiger les risques associés aux informations partagées par erreur.

Mitiger le facteur de risque humain

Dans les films hollywoodiens, les pirates informatiques sont généralement entourés d'écrans et ils tapent sans relâche des lignes de code pour tenter de s'introduire dans un site Web. Cette image est pourtant loin de la réalité. Dans les faits, la plus grande vulnérabilité dans la plupart des organisations est le facteur humain. Plus de 3,4 milliards de courriels d'hameçonnage sont envoyés chaque jour. Si les utilisateurs ne sont pas correctement formés pour les détecter, ce n'est qu'une question de temps avant qu'ils ne tombent dans le piège des cybercriminels.

Conserver un pare-feu à jour, avoir des antivirus solides et posséder une politique stricte en ce qui a trait au matériel informatique sont des éléments essentiels à la cybersécurité. Toutefois, ce sont les personnes qui travaillent avec vous qui comptent le plus. Vos utilisateurs doivent posséder les connaissances adéquates sur les cybermenaces pour les reconnaître et les anticiper, même en situation de vulnérabilité.

Mitiger le facteur de risque humain ne signifie pas pointer les utilisateurs du doigt. Il s'agit plutôt de les outiller pour travailler de façon plus sécuritaire et intelligente. Lorsque vous allez chercher l'appui de la direction, présentez la formation en sensibilisation à la sécurité comme un avantage pour les travailleurs. Il est facile de considérer ce type de formation comme un mal nécessaire, mais elle peut être présentée de manière positive comme une situation où l'employeur fait preuve d'attention et de prévenance envers son personnel.

Les 4 piliers d'une formation en sensibilisation à la sécurité réussie

La sensibilisation à la cybersécurité peut sembler être une tâche ardue. Pourtant, c'est un processus simple une fois décomposé en fonction des différents besoins. Si vous classez les besoins de formation selon les rôles et que vous vous assurez que le contenu est intéressant et adapté à la réalité des utilisateurs, vous serez sur la bonne voie pour favoriser des changements de comportement durables au sein de votre organisation.

1. Du contenu de qualité

Du contenu pertinent et de qualité est essentiel dans tout programme de sensibilisation à la sécurité. Cela permet de motiver les utilisateurs et d'offrir un programme de formation amusant qui interpelle les employés et permet d'améliorer leur comportement pour le mieux.

Voici les cinq facteurs clés qui influencent la qualité du contenu et, ultimement, l'expérience d'apprentissage pour les participants :

1. Le contenu devrait être créé par une équipe d'experts du domaine

Les experts engagés doivent avoir une bonne compréhension des éléments suivants : apprentissage chez l'adulte, psychologie du changement de comportement à long terme, transmission de connaissances, plus récentes tendances en matière de cybersécurité et conformité aux exigences en matière de gouvernance et de confidentialité. Le contenu doit être conçu en interne par le fournisseur sélectionné afin de créer une bibliothèque de cours au ton et à l'aspect uniforme. Cela donne également la possibilité d'être flexible et d'adapter le contenu pour une approche plus personnalisée. Plus d'information sur la personnalisation des campagnes à la page 7.

2. Une approche pédagogique et une méthodologie éprouvée pour l'apprentissage des adultes

La formation en sensibilisation à la sécurité doit être développée en gardant à l'esprit qu'elle s'adresse à des adultes. Elle doit être perçue comme une activité utile de transmission des connaissances et non comme une corvée. Une telle approche est caractérisée par les éléments suivants :

- Le contenu est pertinent et utile. L'accent est mis sur le « pourquoi ».
- L'enseignement est axé sur les tâches à accomplir plutôt que sur la mémorisation
- L'apprentissage autodirigé est conçu pour les adultes, avec des conseils offerts au besoin
- Une navigation contrôlée, principalement linéaire, oblige les participants à avoir des interactions pour avancer et les empêche de passer trop rapidement à travers les sujets
- Un contenu narré et affiché à l'écran (sous-titrage codé) permet de répondre autant aux personnes visuelles qu'auditives
- Des cours personnalisés pour répondre aux exigences culturelles spécifiques
- Une vidéo d'introduction au début de chaque module pour intéresser les participants et introduire le sujet
- Évaluations personnalisables — le nombre de questions, la randomisation et le pointage peuvent être modifiés pour s'adapter aux exigences de chaque organisation

3. Des modules de microapprentissage offrant du contenu spécifique au risque pour renforcer les comportements de sensibilisation à la sécurité

Le microapprentissage est le meilleur format pour provoquer des changements de comportement durables chez les participants. Pour y arriver, assurez-vous que votre contenu :

- Est présenté sous forme de courtes vidéos 2D avec audio
- Se concentre sur un risque, et est proposé sous forme de court format
- Est basé sur des scénarios ramifiés
- Permets aux utilisateurs de prendre des décisions et de voir l'impact immédiat (positif ou négatif) sur la sécurité
- Ne dépasse pas trois minutes

4. La ludification pour stimuler l'intérêt et la motivation

La ludification (gamification) vous permet de maintenir l'engagement des utilisateurs envers le contenu à l'extérieur de l'environnement de formation. Pour développer une approche gamifiée propice aux améliorations en matière de cybersécurité, votre contenu devrait :

- Se baser sur une approche pédagogique pour accroître l'engagement et la motivation
- Compléter l'évaluation du cours et offrir une expérience d'apprentissage positive
- Comprendre un dispositif d'accumulation des points en temps réel, affiché sur un tableau de classement (classement des pairs)
- Faire partie d'une stratégie favorisant la compétition entre les pays, les services ou les rôles
- Offrir une opportunité pour le développement d'initiatives basées sur des mesures incitatives

5. Contenu basé sur les rôles

Les activités d'apprentissage sont conçues en gardant à l'esprit les rôles et responsabilités des participants au sein de l'organisation. La formation est ainsi plus significative et efficace. Voici les catégories d'emploi qui peuvent bénéficier d'un contenu basé sur les rôles en raison du type et de la confidentialité des données auxquelles ils ont accès :

- Gestionnaires
- Administrateurs TI
- Développeurs TI
- Ressources humaines
- Marketing

2. Options de formation personnalisées vs prêtes à l'emploi

Il n'y a pas de réponse parfaite en ce qui a trait à la formation en sensibilisation à la cybersécurité. Les options prêtes à l'emploi et personnalisées ont chacune leurs avantages. Pour identifier la bonne solution pour votre organisation, différents facteurs doivent être considérés.

Les options prêtes à l'emploi sont inégalées en ce qui a trait à la vitesse de déploiement. Si vous êtes confrontés à des défis communs en matière de cybersécurité, une formation clé en main qui aborde les bases de la sensibilisation à la sécurité pourrait s'avérer un choix judicieux. Comme ce type de contenu ne prend que quelques minutes à configurer et à démarrer, cette solution permet à votre organisation de faire preuve de flexibilité et de lancer une campagne de sensibilisation rapidement et facilement.

À garder en tête
Une solution prête à l'emploi est la qualité du contenu. Il faut prendre le temps d'évaluer soigneusement le fournisseur pour s'assurer que les sujets sont bien couverts, et que le contenu est motivant et d'actualité. Comme le contenu ne peut être personnalisé, il doit être particulièrement intéressant pour motiver les utilisateurs à le consulter.

Si vous travaillez dans une grande organisation présente dans plusieurs pays, ou si vous êtes confrontés à des enjeux de cybersécurité particuliers, une campagne personnalisée est probablement la meilleure solution. Qu'il s'agisse de personnaliser l'aspect visuel de la formation, le contenu ou la langue, une campagne personnalisée de sensibilisation à la sécurité vous offre une grande liberté.

Cette option vous procure une flexibilité maximale concernant le contenu et sa distribution. Elle vous permet également d'aborder des questions propres à votre entreprise et d'offrir le contenu le plus à jour possible en tenant compte des plus récentes tentatives de cyberattaque.

3. Options de formation basées sur les risques et sur les rôles

Lorsque vous planifiez une campagne de sensibilisation à la cybersécurité, deux options s'offrent à vous. Le contenu peut être ciblé en fonction du type de risque ou du rôle. La première option vise à lutter contre les problèmes spécifiques à votre organisation, comme l'hameçonnage ou les attaques liées au mot de passe. La deuxième se concentre sur les enjeux propres à chaque service, comme les fausses factures pour le service de comptabilité ou l'ingénierie sociale pour la direction.

Ces deux options peuvent être utilisées dans une stratégie autonome, mais elles sont plus efficaces lorsque combinées. Un enjeu comme l'hameçonnage comporte plusieurs facettes et peut avoir différentes implications selon les services ou même le niveau hiérarchique. En combinant ces deux éléments, vous obtenez une meilleure compréhension des enjeux auxquels fait face votre organisation.

Voici les services qui risquent davantage d'être confrontés à des cyberattaques spécialisées :

Gestionnaires

Plus de personnes et de ressources financières sont impliquées, plus le risque associé à la cybersécurité est grand. À ce niveau, les utilisateurs ont accès à des fonds et à des données sensibles appartenant à l'entreprise.
Il est donc nécessaire de se protéger de l'ingénierie sociale. Les utilisateurs devraient participer à quelques simulations d'hameçonnage et apprendre comment détecter les fausses factures afin de prévenir le partage involontaire d'authentifiant.

Développement des TI

Les entreprises se fient de plus en plus sur les développeurs pour gérer des aspects essentiels de leurs affaires ou concevoir des produits. Ces employés constituent des cibles fréquentes en raison de leur accès à des données critiques. Le contenu de formation à leur proposer devrait donc être axé sur des menaces comme les rançongiciels.

Marketing/RH

Les pirates ciblent souvent ces services parce qu'ils utilisent une variété d'applications dans le cadre de leurs activités quotidiennes. Il y a donc plus de risques liés à la faiblesse des mots de passe ou à leur réutilisation. Les conséquences d'une brèche peuvent être dévastatrices, en particulier dans le cas des RH qui manipulent des informations personnelles, comme les numéros d'assurance sociale. Il est essentiel d'offrir à ces services une formation sur la sécurité des mots de passe, ainsi que des simulations d'hameçonnage impliquant une fausse demande de réinitialisation du mot de passe.

4. Simulations d'hameçonnage réalistes

Les simulations d'hameçonnage constituent une part essentielle de toute campagne de formation en sensibilisation à la cybersécurité. L'hameçonnage est l'un des types de cyberattaques les plus fréquents, et il peut prendre un nombre alarmant de formes différentes. Vos utilisateurs doivent savoir reconnaître et combattre ces attaques, qu'il s'agisse d'ingénierie sociale ou d'un faux site Web.

Voici les éléments essentiels d'une simulation d'hameçonnage réussie :

Tentatives multiples

Ne vous limitez pas aux types d'attaques les plus communes, ou à celles qui ont frappé votre organisation. Proposez des tentatives d'ingénierie sociale différentes, comme un simple courriel, une fausse page de connexion ou le téléchargement d'un logiciel malveillant, pour vous assurer que les utilisateurs demeurent sur le qui-vive. Cela vous permettra également de recueillir suffisamment de données sur vos besoins.

Analyse des données

La plateforme de simulation d'hameçonnage choisie doit inclure une fonctionnalité intégrée d'analyse des données. Ces simulations seront utilisées pour identifier les types de contenu à approfondir et pour évaluer la réussite de la campagne au cours de l'année. C'est pour cette raison que la collecte de données détaillées est importante. Elle permet aussi bien d'obtenir les résultats d'un utilisateur particulier que d'identifier les tendances globales à travers l'entreprise.

Outils de suivi de qualité

Une fois les simulations d'hameçonnage réalisées et les données compilées, il est temps de passer à l'action. Les outils utilisés à la suite d'une simulation d'hameçonnage devraient être diversifiés et peuvent être utilisés pour l'atteinte de divers objectifs. Les outils les plus communs sont une infolettre précisant les résultats de la simulation et une formation vidéo présentant les plus récentes tendances en matière d'hameçonnage.

Meilleures pratiques

Planifier les campagnes et concevoir les cours selon une approche d'apprentissage automatisée fondée sur les résultats, comprenant la formation de base, le microapprentissage, les simulations d'hameçonnage et la formation juste à temps.

Définir une stratégie de sensibilisation sur mesure pour tenir compte des besoins d'apprentissage propres aux différents groupes (p. ex. nouvelles recrues, champions, cliqueurs en série, etc.)

Identifier les objectifs de sensibilisation à la sécurité qui vous aideront à obtenir l'approbation et l'appui de la direction pour votre programme.

Déterminer les paramètres et les indicateurs clés de performance qui vous aideront à mesurer le succès de votre programme et à ajuster les objectifs pour appuyer la stratégie et la mission de votre entreprise.

Choisir un partenaire visionnaire

Pour votre formation en sensibilisation à la cybersécurité, choisissez un partenaire visionnaire plutôt qu'un simple fournisseur. Recherchez une entreprise qui met de l'avant une approche consultative, et qui prendra le temps de comprendre votre situation unique et d'anticiper vos besoins. Le bon partenaire possède l'expérience et l'expertise technique pour vous aider à planifier et à mettre en œuvre un programme de sensibilisation à la sécurité conçu spécifiquement pour votre organisation.

Le bon fournisseur ira au-delà de vos données historiques. Il sera en mesure de les extrapoler pour prédire vos besoins et vous aider à élaborer une stratégie qui vous permettra d'accroître sans cesse le niveau de sensibilisation à la cybersécurité au sein de votre organisation.

En faisant appel à un partenaire, vous avez accès à une équipe d'experts qui possède les connaissances nécessaires pour évaluer et analyser les données, et ainsi optimiser votre programme de sensibilisation à la sécurité. N'oubliez pas, vous n'êtes pas seul !

Un partenaire visionnaire en sensibilisation à la sécurité :

- Offre des conseils d'expert et de l'encadrement pour planifier et mettre en œuvre votre programme de sensibilisation à la sécurité. Un partenaire devrait présenter une feuille de route impressionnante dans ce domaine et avoir établi de nombreux programmes de sensibilisation à la sécurité. Il est également en mesure de comprendre les éventuels obstacles, d'anticiper les défis et d'être disponible pendant vos campagnes.
- Fournis une expertise et la transmission de connaissances pour optimiser vos programmes, motiver les utilisateurs et favoriser les changements de comportement.
- Travaille avec vous pour recueillir les données et évaluer les résultats, déterminer les forces et les succès et identifier les pistes d'amélioration.
- Utilise une approche pédagogique et une méthodologie éprouvée pour l'apprentissage en ligne des adultes.

Conclusion

Dans le cadre du plus récent Gone Phishing Tournament organisé par Terranova Security, plus de 190 000 participants ont cliqué sur un lien contenu dans un courriel d'hameçonnage. Les principes pédagogiques simples présentés dans ce guide peuvent contribuer à réduire ce chiffre impressionnant. La formation en sensibilisation à la cybersécurité n'a pas à être intimidante.
Les principes de base sont simples :

Soyez intéressant. Proposez du contenu pertinent et de qualité pour conserver l'intérêt de vos utilisateurs.

Restez vigilant. Chaque jour voit la naissance d'une nouvelle technique d'hameçonnage ou d'un nouveau virus. Pour vous en prémunir, il est primordial de continuellement améliorer la formation en sensibilisation à la cybersécurité.

Amusez vos utilisateurs. Il y a une raison pour laquelle les gens se souviennent des moindres détails de leur jeu vidéo préféré. C'est parce qu'ils ont eu du plaisir et qu'ils ont été récompensés pour leur participation. Qu'il s'agisse de points, d'un tableau de classement ou de médailles, donnez à vos utilisateurs des raisons supplémentaires de suivre la formation.

Mettez-vous à leur place. Chaque personne a une réalité différente, et cela devrait se refléter dans la formation en sensibilisation à la cybersécurité. Évaluez les besoins de chaque utilisateur en fonction de son rôle, sans quoi vous vous retrouverez avec des méthodes inefficaces.

Soulignez les avantages. La formation en sensibilisation à la cybersécurité est souvent considérée comme une corvée, alors qu'il s'agit d'une opportunité de développement personnel et professionnel. Les ordinateurs constituent une partie essentielle de nos vies. Vos utilisateurs devraient posséder la formation appropriée pour comprendre les risques qu'ils encourent et font courir à leur entreprise et les meilleures pratiques associées à la réduction de ces risques.

La formation en sensibilisation à la sécurité constitue un investissement important pour l'évolution de votre organisation. En suivant ces cinq conseils simples, vous serez sur la voie du succès.

Découvrez les atouts d'une formation en sensibilisation à la cybersécurité et la différence qu'elle peut faire pour vous !

PLANIFIER UNE DÉMO DÈS MAINTENANT

FORTRA

WWW.TERRANOVASECURITY.COM/FR