awaretrain
Security Awareness

Livre blanc

Qu'est-ce qui fait le succès d'une campagne de sensibilisation et pourtant pourquoi échouent-elles souvent ?

awaretrain.fr

L'objectif d'une campagne de sensibilisation à la sécurité est de créer un environnement de travail sûr dans lequel les employés sont conscients de leur rôle et de leurs responsabilités en matière de sécurité de l'information et de cybersécurité. Pour y parvenir, il ne suffit pas de fournir des informations sur les risques et d'expliquer le comportement à adopter. Premièrement, les personnes doivent être en mesure de comprendre et d'appliquer les conseils et, deuxièmement, ils doivent avoir la volonté de comprendre et d'appliquer ces conseils. Cela nécessite un changement d'attitude et d'intention.

Dans ce livre blanc, nous développons six points qui, sur la base de notre propre expérience, sont essentiels à la réussite d'une campagne de sensibilisation à la sécurité. En outre, cette expérience nous a également appris pourquoi certaines campagnes ne donnent pas les résultats escomptés.

Points essentiels pour une campagne réussie

1. Communication interne

Un bon départ, c'est la moitié de la bataille. Un programme de sensibilisation réussi commence par la manière dont il est annoncé au sein de l'organisation. Suscitez l'adhésion des employés en incluant une vidéo dans laquelle la direction explique la nécessité du programme. Utilisez des outils de communication interne tels que des « Newsletter » et des messages sur l'intranet pour tenir les employés informés de certaines actions et de ce à quoi ils doivent s'attendre. Vous pouvez également utiliser des affiches et des dessins humoristiques en rapport avec le sujet afin d'accroître l'engagement des employés. Notre conseil : impliquez le service de communication interne dans la campagne !

« Impliquez le service de communication dans la campagne ! »

2. Formation assistée par ordinateur

La majorité des employés ont accès à un ordinateur. C'est pourquoi nous recommandons toujours de faire de la formation assistée par ordinateur (également connue sous le nom d'apprentissage en ligne) un élément important d'un programme de sensibilisation à la sécurité. Cela s'explique en partie par son évolutivité, son accessibilité et la possibilité pour les employés de suivre la formation à leur propre rythme. Les enquêtes menées auprès des employés montrent que les formations en ligne basées sur la vidéo sont préférées aux jeux et aux formations basées sur le texte. La combinaison d'un

texte parlé et d'images visuelles a un impact positif sur l'effet d'apprentissage et augmente l'intention de vouloir apprendre.

3. Réunions physiques

Des réunions et des événements bien organisés permettent de donner vie au sujet au sein de l'organisation et d'impliquer davantage les employés dans la sécurité de l'information. Par le biais d'une telle séance d'information, vous pouvez faire comprendre pourquoi le sujet doit être abordé. Aujourd'hui, un webinaire est bien sûr une excellente alternative.

« Des événements bien organisés rendent le sujet plus vivant. »

4. Tout est facilement accessible

Réduire les obstacles qui empêchent les employés de trouver les bonnes informations. Un système généralement accessible sert de base de connaissances, où toutes les informations nécessaires peuvent être trouvées sur les différents sujets relatifs à la sécurité de l'information, à la cybersécurité et à la protection de la vie privée. En plus d'appliquer l'apprentissage aux situations de travail, il est également très important de fournir des informations et des conseils sur des situations privées, telles que la sécurisation des comptes de médias sociaux et la protection des enfants en ligne.

5. Tester le comportement et créer des moments propices à l'apprentissage

Les simulations d'hameçonnage et les enquêtes d'ingénierie sociale, sont des moments propices à l'apprentissage et démontrent la nécessité de la campagne. Permettre aux employés de faire l'expérience des risques augmentera leur volonté d'apprendre. Incorporez les résultats dans un discours d'ouverture. Cela renforcera l'importance du sujet.

Mais attention. Ces simulations requièrent une certaine prudence. Vous ne voulez pas créer une culture de la peur et vous ne voulez pas que les gens la perçoivent comme du harcèlement. Un bon exemple est celui d'un test de phishing de l'une des plus grandes banques néerlandaises il y a quelques années. Ils ont envoyé un e-mail de phishing avec un message joyeux sur le retour du cadeau de Noël supprimé de l'année d'avant. Cela a choqué de nombreux employés et a ainsi créé un effet contreproductif.

« Les employés seront plus enclins à apprendre s'ils ont l'occasion de faire l'expérience des dangers. »

6. Utilisez la langue de l'employé

Ce qui semble à première vue être un manque de motivation peut en fait être un manque de capacité d'apprentissage. Il appartient aux formateurs, développeurs et autres professionnels de la sensibilisation à la sécurité de traduire des documents complexes en leçons faciles à comprendre et en outils pratiques pouvant être appliqués immédiatement.

Pourquoi certaines campagnes échouent de toute façon

1. Les employés ne comprennent pas ce que signifie réellement la sensibilisation à la sécurité

Pour que les employés comprennent ce que signifie la sensibilisation à la sécurité, les informations doivent être transmises d'une manière qui corresponde à la façon dont les gens pensent et agissent dans la pratique. Les gens doivent être capables de se reconnaître dans les situations et de comprendre comment les connaissances qu'ils acquièrent impactent leurs actions. La sensibilisation à la sécurité est une discipline exigeante. Un bon professionnel de la sensibilisation à la sécurité fixe des objectifs et peut traduire le sujet correctement pour l'employé. Il sait également comment utiliser différentes méthodes d'apprentissage pour sensibiliser et changer les comportements.

« Allez au-delà du simple fait de cocher une case. »

2. Pouvoir cocher une case

Nous rencontrons régulièrement des organisations qui ne s'occupent de la sensibilisation à la sécurité que pour "cocher la case" indiquant qu'elles ont fait quelque chose pour sensibiliser les employés. Il suffit d'envoyer un courrier interne contenant des informations et des conseils ou d'organiser un cours de formation ponctuel. En tant qu'organisation, vous aurez effectivement fait quelque chose en matière de sensibilisation à la sécurité, mais vous ne réaliserez absolument aucun changement de comportement et vous ne créerez certainement pas un environnement de travail durable et conscient de l'importance de l'information. Par conséquent, allez au-delà de cocher une case.

3. Cela ne devrait pas prendre trop de temps

L'efficacité d'un programme est déterminée par les ressources que vous lui allouez en tant qu'organisation. Il y a une grande différence entre une action ponctuelle et un processus continu de sensibilisation avec différentes méthodes et mesures d'apprentissage. Nous voyons souvent des organisations considérer la sensibilisation à la sécurité comme une action ponctuelle. Ils pensent que le changement peut se produire avec une seule simulation de phishing.

4. Manque de matériel d'apprentissage attrayant, varié et approprié

Le simple fait d'informer sur un sujet ou des risques spécifiques ne constitue pas une formation. Pensez aux formations en ligne basées sur des textes. Il faut aller plus loin pour capter et retenir l'intérêt des employés. Proposez des méthodes d'apprentissage variées et rendez le processus d'apprentissage interactif.

5. Absence de suivi du programme

En mesurant régulièrement les niveaux de sécurité et en surveillant les progrès et les résultats des employés, vous pouvez ajuster le programme si nécessaire. Vous pouvez également déterminer quelles méthodes d'apprentissage fonctionnent ou non au sein de l'organisation. Pour obtenir l'image la plus complète possible, nous vous recommandons d'effectuer une mesure de référence, une mesure intermédiaire par le biais de simulations d'hameçonnage ou d'autres enquêtes d'ingénierie sociale et une mesure d'évaluation.

6. Attentes déraisonnables

Aucune mesure de sécurité de l'information ne garantira une sécurité à 100%. Il ne faut donc pas s'attendre à ce que tous les incidents puissent être évités. Un moment d'inattention et une erreur est facilement commise. En outre, les criminels développent constamment de nouvelles techniques et méthodes pour tromper les gens. Donc, la sécurité à 100% n'est pas possible, mais vous pouvez grandement minimiser les risques d'incidents.

Conclusion

Une campagne de sensibilisation à la sécurité réussie consiste en une combinaison de méthodes d'apprentissage. Il n'existe pas de méthode d'apprentissage unique qui soit par définition la meilleure. C'est le renforcement entre les ressources et la façon dont l'histoire est racontée qui déterminent le succès d'une campagne de sensibilisation à la sécurité. Notre conseil est de considérer la sensibilisation à la sécurité non pas comme une action ponctuelle, mais comme un processus continu. Prenez en compte la langue de l'employé, rendez la campagne interactive et surtout, soyez créatif. Vous pouvez déjà faire beaucoup vous-même pour renforcer le sujet !

Découvrez la plateforme Awaretrain

Rejoignez les organisations qui utilisent notre plateforme de sensibilisation à la sécurité. Notre plateforme est l'outil idéal pour faire passer la sensibilisation à la sécurité des employés à un niveau supérieur. Notre bibliothèque de contenu* contient plus de 50 modules de formation interactifs et ludiques sur un large éventail de sujets relatifs à la sécurité de l'information, à la cybersécurité et à la protection de la vie privée. En outre, il est possible d'envoyer des simulations de phishing via la plateforme.

**** Contenus intégrables dans des LMS.***

Essayez-la pendant 28 jours gratuitement !

→ Demandez votre compte de test

Contactez-nous

+33 (0)1 44 04 01 73

info@awaretrain.fr

awaretrain.fr

awaretrain
Security Awareness