FORTRA™

GUIDE (TERRANOVA SECURITY)

La gamification : pour une formation en sensibilisation à la sécurité réussie

Réduire le risque humain lié aux cybermenaces

TABLE DES MATIÈRES

SOMMAIRE

La formation en sensibilisation à la cybersécurité en milieu de travail doit changer. Les employés sont occupés à gérer de nombreux livrables et leur intérêt à participer à des séances de formation corporatives est minime.

La ludification, ou gamification, propose aux employés une formation pertinente, engageante, motivante et intéressante. Lorsqu'elle est utilisée dans le cadre d'un programme corporatif de sensibilisation à la cybersécurité suivant une méthode de formation éprouvée basée sur la science, la gamification permet d'atteindre un niveau supérieur d'apprentissage.

Les entreprises ne peuvent pas se permettre de simplement espérer que leur formation en sensibilisation à la cybersécurité fonctionne. Les leaders en sensibilisation à la sécurité doivent utiliser des résultats mesurables, des mécanismes de surveillance et des modules de formation réactifs pour évaluer le succès de la formation.

L'être humain a une tendance naturelle à faire confiance, à croire que chacun est foncièrement bon. Il lui est difficile de concevoir que quelqu'un pourrait le voler ou le tromper délibérément.

Malheureusement, c'est très loin d'être la réalité. La plus grande menace à la cybersécurité est d'origine humaine. Les attaques d'hameçonnage, y compris les courriels, messages textes et messages vocaux malveillants, coûtent en moyenne 1,1 million $ aux entreprises.

Lorsqu'il s'agit de cybersécurité, les personnes représentent le plus grand facteur de risque pour les entreprises. Toutefois, ces mêmes personnes peuvent également constituer un atout puissant pour défendre les entreprises contre les menaces de cybersécurité.

Une formation centrée sur les personnes permet aux entreprises de développer une culture de cybersécurité éprouvée. Les employés demeurent vigilants et sont en mesure de détecter les cybercriminels qui utilisent des techniques astucieuses d'ingénierie sociale pour voler, tromper et duper.

Le désir humain de faire confiance est toujours présent, mais en comprenant mieux la façon dont les cybercriminels opèrent, les employés sont en mesure de se protéger, eux et leur organisation.

L'un des défis réside dans le fait que le respect des règles et la formation en sensibilisation à la sécurité sont des sujets qui peuvent être perçus comme étant sérieux et arides. Malgré un contenu parfait, les gens ne s'intéressent tout simplement pas à la formation. En leur for intérieur, une majorité d'entre eux continuent à croire que cela « ne leur arrivera pas ».

C'EST ICI QU'ENTRE EN JEU LA GAMIFICATION.

Cyberdéfi - Voyager en toute sécurité

Malheureusement, c'est très loin d'être la réalité. La plus grande menace à la cybersécurité est d'origine humaine. Les attaques d'hameçonnage, y compris les courriels, messages textes et messages vocaux malveillants, coûtent en moyenne

1,1 million $ aux entreprises

Cyberdéfi - Services en nuage

Motiver et engager grâce à la gamification

Gartner définit la gamification de la façon suivante :

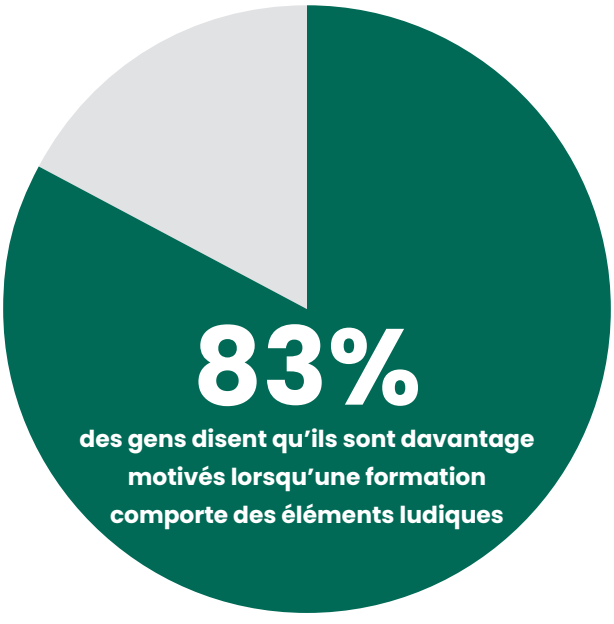
La gamification est l'utilisation de mécaniques de jeu pour susciter l'engagement dans des scénarios liés au travail. L'objectif est de changer les comportements du public cible pour atteindre les résultats ciblés par l'entreprise. Plusieurs types de mécaniques peuvent être utilisées pour rendre le jeu plus agréable, comme des pointages, des défis, des tableaux de classement, des règlements et des incitatifs. La gamification applique ces stratégies pour motiver les participants à atteindre des niveaux plus élevés et significatifs d'engagement. Les humains sont « programmés » pour apprécier les jeux. Ils ont tendance à interagir davantage dans les activités construites sur ce modèle.

Cette approche à la formation en cybersécurité et à la sensibilisation est puissante. Les participants sont engagés, intéressés et activement motivés à continuer leur apprentissage.

La gamification fait vivre aux participants des scénarios réalistes qui permettent de faire des liens directs entre une action et son impact sur la sécurité des collègues et de l'organisation.

Lorsque la gamification est utilisée dans le cadre d'un programme de formation en sensibilisation à la cybersécurité, les participants peuvent constater d'eux-mêmes la pertinence et l'applicabilité de leurs apprentissages au quotidien.

- 83 % des gens disent qu'ils sont davantage motivés lorsqu'une formation comporte des éléments ludiques
- Le niveau d'ennui en lien avec la formation chute à 10 %
- 33 % des gens veulent davantage de jeux dans leurs formations



La gamification favorise les apprentissages mesurables

L'apprentissage passe par l'action. Les gens veulent faire quelque chose, l'essayer, le tester. Ils veulent gagner et voir leurs résultats. C'est ce que permet la gamification de la formation en cybersécurité.

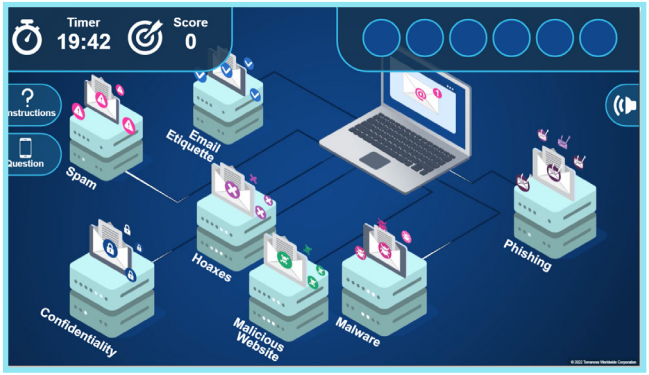
La motivation des gens passe par la constatation de leur réussite, la récolte de médailles, la résolution de problèmes et l'atteinte du sommet du tableau de classement. En proposant une formation mesurable et engageante, les employés auront tendance à discuter entre eux des défis de la formation, à comparer leurs résultats et à échanger sur leurs apprentissages.

Exemple d'un tableau de classement gamifié sur la plateforme de sensibilisation à la sécurité de Terranova Security.

Pendant la formation, et selon ses réponses, l'utilisateur accumule des points de gamification compilés dans SCORM. Au fur et à mesure que chaque activité est complétée, les points s'accumulent et sont affichés sur le tableau de classement.

La gamification de la formation en cybersécurité favorise le développement et la promotion d'une culture de sensibilisation à la cybersécurité. Les employés connaissent les risques réels que représentent l'hameçonnage, les maliciels, le BEC et les autres cybermenaces. Ils comprennent comment leur proactivité face aux cybermenaces peut les protéger, eux, leurs collègues et leur organisation.

Toutefois, il ne suffit pas de simplement ajouter des graphiques interactifs ou d'accorder des médailles pour avoir compléter la formation.



Cyberdéfi - Courriel

Impacts réels de l'ingénierie sociale

Les gens doivent créer un lien émotionnel entre la formation et leur travail. Ils doivent comprendre quelles peuvent être les conséquences de ne pas lire leurs courriels avec attention, de ne pas scruter chaque adresse courriel à la loupe ou de ne pas remettre en doute une demande urgente de transfert de fonds.

Pour y parvenir efficacement, la gamification doit faire partie d'une plateforme plus large de sensibilisation à la cybersécurité. Il est essentiel qu'une plateforme de sensibilisation à la sécurité propose un éventail de types de formations, y compris des cours modulaires, des outils de simulation d'hameçonnage, du microapprentissage, de la gamification et des outils de communication corporatifs.

Enfin, pour mesurer les apprentissages, cette plateforme doit être couplée à une capacité à suivre les taux de succès des employés, leurs niveaux d'engagement et les points à améliorer. Des formations supplémentaires en sensibilisation à la cybersécurité sont également à prévoir.

Les gens sont motivés par la rétroaction. C'est exactement ce que permet la gamification. Elle donne aux leaders et aux employés une rétroaction directe sur les taux d'engagement, les niveaux de réussite et les points à améliorer.

« La gamification s'appuie sur des principes soutenus par la recherche. Les concepts de motivation des apprenants, d'apprentissage distribué et de récupération espacée utilisés dans la gamification ont permis d'obtenir des résultats positifs. Ce n'est pas de la poudre aux yeux. Cette méthode est basée sur une méthodologie scientifique solide. »

Cyberdéfi - Cycle de vie de l'information

Pourquoi la gamification?

La gamification permet d'augmenter la motivation des employés face à la formation en sensibilisation à la cybersécurité. Aucune entreprise ne peut se permettre d'avoir en son sein des employés démobilisés. Le risque est trop grand.

Les formations sous forme de présentations, de déjeuners-conférences ou de courriels corporatifs ne fonctionnent pas. Par expérience, les employés les trouvent ennuyantes et non pertinentes. La gamification change le paradigme d'apprentissage en démontrant aux participants que les cyberattaques représentent un risque réel et qu'ils doivent savoir quoi faire pour se protéger, et protéger l'organisation.

La gamification offre les éléments suivants :

1. Engagement

Lorsque la gamification est bien utilisée, elle donne aux participants un but à atteindre. Ils comprennent pourquoi ils suivent la formation et peuvent être fiers de leur niveau de réussite.

2. Changement de comportement

La clé pour construire une culture de cybersécurité passe par le changement de comportement. Lorsque les employés comprennent comment leurs actions affectent l'organisation, ils sont plus susceptibles d'apprendre et de changer.

3. Rétroaction instantanée

Les gens sont motivés par la réussite. Quand ils parviennent à relever un défi de cybersécurité et obtiennent un maximum de points, ils se sentent compétents et sont motivés à continuer l'apprentissage. La gamification rend les employés plus confiants quant à leurs connaissances en cybersécurité. Ils sont ainsi plus à même de participer à des programmes d'apprentissage avancé et à devenir des cyberhéros.

4. Rétention des connaissances

L'apprentissage passe par l'action et la répétition. Des techniques de gamification astucieuses utilisent différents formats pour renforcer les messages clés, favorisant un apprentissage intrinsèque. La recherche montre que le taux de rétention pour les formations à participation active est de 75 %, comparativement à 20 % pour les approches d'apprentissage passives traditionnelles.

5. Environnement d'apprentissage sécuritaire

Dans un environnement de formation gamifié, le téléchargement d'une pièce jointe ou l'ouverture d'un courriel d'hameçonnage n'entraîne pas de conséquences graves. Les participants constatent d'eux-mêmes comment leurs décisions peuvent avoir un impact sur eux et leur entourage, sans répercussions négatives. La clé est de donner aux employés l'occasion de repasser à travers la formation afin qu'ils puissent appliquer directement les leçons apprises dans un environnement sécuritaire. Dans un environnement de formation gamifié, le téléchargement d'une pièce jointe ou l'ouverture d'un courriel d'hameçonnage n'entraîne pas de conséquences graves. Les participants constatent d'eux-mêmes comment leurs décisions peuvent avoir un impact sur eux et leur entourage, sans répercussions négatives. La clé est de donner aux employés l'occasion de repasser à travers la formation afin qu'ils puissent appliquer directement les leçons apprises dans un environnement sécuritaire.

Il n'est pas facile de convaincre les employés de se soucier de la cybersécurité. Les entreprises doivent considérer des approches de formation modernes, pertinentes, intéressantes et efficaces, qui vont au-delà de la méthodologie traditionnelle.

Cinq questions sur la gamification et la formation en sensibilisation à la cybersécurité

Lorsqu'ils évaluent les options de formation en sensibilisation à la cybersécurité, les leaders et les décideurs doivent se poser les cinq questions suivantes avant de prendre une décision :

1. Y A-T-IL DES RÈGLEMENTS?

Les règlements permettent de contrôler les participants et de guider la prise de décisions. Assurez-vous qu'il est possible d'établir des règles en fonction des objectifs propres à la formation. Une fois ces règlements ou objectifs définis, la formation gamifiée a un but et une valeur. Établissez des règlements simples, qui permettent aux employés de se concentrer sur l'apprentissage.

2. COMMENT LE CHANGEMENT DE COMPORTEMENT EST-IL FAVORISÉ?

Les formations qui récompensent les participants avec des points, des médailles, des tableaux de classement ou des prix réels contribuent au changement de comportement. Il est prouvé scientifiquement que lorsqu'on gagne, le cerveau libère de la dopamine, ce qui crée un effet de plaisir. Les participants sont donc encouragés à continuer, à progresser et à mettre en pratique le comportement pour lequel ils ont été récompensés dans le cadre de leur formation.

3. EST-ELLE FLEXIBLE ET PERSONNALISABLE?

Il n'existe pas deux entreprises pareilles. Les formations uniques ne fonctionnent pas. Assurez-vous que les caractéristiques de gamification peuvent être modifiées en fonction des besoins des employés. De plus, la méthode de marquage des points est propre à chaque culture d'entreprise – certains employés peuvent être plus à l'aise avec un système de pointage privé plutôt qu'avec un tableau de classement partagé et public. Les leaders et décideurs doivent garder le contrôle sur la façon dont la formation s'insère dans la culture et les objectifs généraux de l'entreprise.

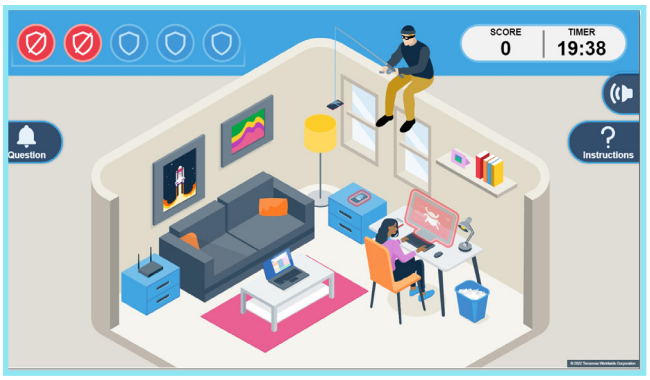
4. LA FORMATION EST-ELLE ACTIVE OU PASSIVE?

L'erreur humaine et l'inattention sont à blâmer pour la majorité des attaques de cybersécurité. Les entreprises ne peuvent pas se permettre de laisser l'inattention et l'ennui être le statu quo de la formation en cybersécurité. Avec la gamification, les employés doivent interagir, s'engager et prendre des vraies décisions avant de pouvoir progresser vers le prochain segment de formation. L'apprentissage actif permet aux participants d'apprendre par l'action.

5. QUEL EST LE MODE D'ENGAGEMENT ET D'ENSEIGNEMENT?

Le facteur risque est déterminant dans la formation. Lorsque les gens ont peur de faire des erreurs, de répondre à des questions directes ou même de poser des questions qui peuvent paraître « idiotes », l'apprentissage et l'engagement stagnent. En intégrant la gamification à une plateforme de sensibilisation à la sécurité, on élimine le risque. Les participants peuvent travailler sur les modules d'apprentissage à leur propre rythme, faire des erreurs, et avoir l'occasion de refaire des segments pour accroître leur confiance et leurs connaissances.

Cyberdéfi - Appareils mobiles



Cyberdéfi - Protéger votre bureau à domicile

Mobiliser les employés pour créer une culture de sensibilisation à la cybersécurité

Ce n'est pas un secret. Les employés heureux sont engagés, motivés et se sentent plus connectés aux objectifs corporatifs. Ces employés constatent comment leurs actions font partie de la croissance et du progrès général de l'entreprise.

Ces personnes voient clairement comment elles s'insèrent dans les réussites de leurs collègues et de l'organisation. Elles sentent qu'elles font partie de quelque chose de plus grand.

C'est cette réaction émotionnelle exacte qu'un programme de cybersécurité corporatif doit générer. Chaque employé doit être connecté au message et comprendre comment il peut contribuer à la sécurité de l'entreprise.

Les formations en cybersécurité réalistes, qui utilisent la gamification, des outils de simulation et des modules d'apprentissage stratégiques, contribuent à maintenir l'engagement, la stimulation et la connexion des employés. Les participants comprennent immédiatement les dangers de l'ingénierie sociale, de l'hameçonnage, des maliciels, du BEC et d'autres cybermenaces.

La gamification permet d'expérimenter les impacts concrets d'une cyberattaque, ce qui crée une connexion émotionnelle au risque. Cela contribue à stimuler la communication et à favoriser le déploiement d'une culture de sensibilisation à la sécurité favorable et connectée.

Les entreprises récoltent une culture de sensibilisation à la cybersécurité qui encourage l'apprentissage et le développement de cyberhéros. Au final, les employés sont engagés, motivés et performants.

Références

https://www.techrepublic.com/article/cyberattacks-now-cost-businesses-an-average-of-1-1m/

https://www.gartner.com/it-glossary/gamification-2

https://elearningart.com/blog/gamification-tips-karl-kapp/

https://www.talentlms.com/blog/gamification-survey-results/

https://www.educationcorner.com/the-learning-pyramid.html

Découvrez comment la sensibilisation à la sécurité centrée sur les personnes continue à former des millions de cyberhéros, à changer des comportements et à instiller une culture de sécurité à travers le monde

DEMANDER UNE DÉMO

FORTRA™

Fortra.com

À propos de Fortra

Fournisseur de logiciels de cybersécurité unique sur le marché, Fortra propose à ses clients un futur à la fois plus simple et plus résilient. Nos experts et notre portefeuille, riche de solutions évolutives et intégrées, offrent aux entreprises du monde entier une maîtrise et un équilibre accrus. Acteurs du changement positif, nous vous accompagnons à chaque étape de votre parcours de cybersécurité et vous aidons à garder l'esprit serein. Pour en savoir plus, rendez-vous sur fortra.com/fr.

(fta-tn-gd-0424-r1-79d)