Programmes de formation sur ordinateur pour tous les niveaux de l'entreprise

Kaspersky Security Awareness

kaspersky BIENVENUE DANS LE FUTUR

Plus d'informations sur kaspersky.fr

Kaspersky Security Awareness

Un moyen efficace de développer une culture de la cybersécurité au sein de votre entreprise

Plus de 80 % des incidents informatiques sont dus à l'erreur humaine. Une culture de la cybersécurité ainsi que des compétences fondamentales et une sensibilisation à la cybersécurité dans toute votre organisation sont essentielles pour réduire la surface d'attaque et le nombre d'incidents auxquels vous devez faire face. Les organisations ont souvent du mal à trouver les bons outils et les bonnes méthodes pour former efficacement leurs employés afin d'améliorer leur comportement. La clé de la réussite consiste à déployer une formation qui utilise les dernières techniques et technologies en matière d'éducation des adultes et qui offre le contenu le plus pertinent et le plus actuel.

Le facteur humain est l'élément le plus vulnérable de la cybersécurité
Les solutions de cybersécurité se développent et s'adaptent rapidement à des menaces complexes, compliquant la tâche des cybercriminels qui se tournent vers l'élément le plus vulnérable de la cybersécurité : le facteur humain.

52 % des entreprises considèrent les employés comme la principale menace pour la cybersécurité en entreprise*

60 % des employés ont des données confidentielles sur leur appareil professionnel (données financières, base de données de messagerie, etc.)**

30 % des employés reconnaissent qu'ils partagent l'identifiant et le mot de passe de leur PC professionnel avec des collègues**

23 % des organisations n'ont mis en place aucune règle ni politique de cybersécurité pour le stockage de données d'entreprise**

Kaspersky Security Awareness : une nouvelle approche pour maîtriser les compétences en matière de sécurité informatique

Kaspersky Security Awareness offre une gamme de solutions de formation très intéressantes et efficaces qui renforcent la sensibilisation à la cybersécurité de votre personnel afin que celui-ci contribue pleinement à la cybersécurité de votre organisation. Étant donné que les changements durables de comportement prennent du temps, notre approche consiste à mettre en place un cycle d'apprentissage continu qui englobe différents modules.

Cycle d'apprentissage continu

Engagement/ Motivation	Point de départ	Apprentissage	Renforcement
– Pourquoi ai-je besoin de cela ? – Connaissance	– En suis-je conscient ? – Que sais-je et où sont les lacunes ?	– Micro-apprentissage – Formation continue – Adaptativité	– Ai-je bien compris ? – Est-ce que je m'en souviens ? – Est-ce que j'agis en conséquence ?

Principaux facteurs de différenciation des programmes

Une expertise considérable en matière de cybersécurité

Plus de 20 ans d'expérience dans le domaine de la cybersécurité transformés en un ensemble de compétences de cybersécurité qui est au cœur de nos produits.

Des formations qui modifient le comportement des employés à chaque niveau de votre organisation

Notre formation ludique stimule l'intérêt et la motivation grâce au divertissement éducatif, tandis que les plateformes d'apprentissage permettent d'internaliser les compétences en matière de cybersécurité afin de s'assurer que les compétences acquises ne se perdent pas en cours de route.

* Étude : « The cost of a data breach » (Le coût d'une violation de données), Kaspersky Lab, printemps 2018.

** « Sorting out a Digital Clutter » (Mettre de l'ordre dans le fouillis numérique). Kaspersky Lab, 2019.

Les employés commettent des erreurs. Les entreprises perdent de l'argent…

1 195 000 $
par entreprise
Impact financier moyen des violations de données causées par une mauvaise utilisation des ressources informatiques par les employés*

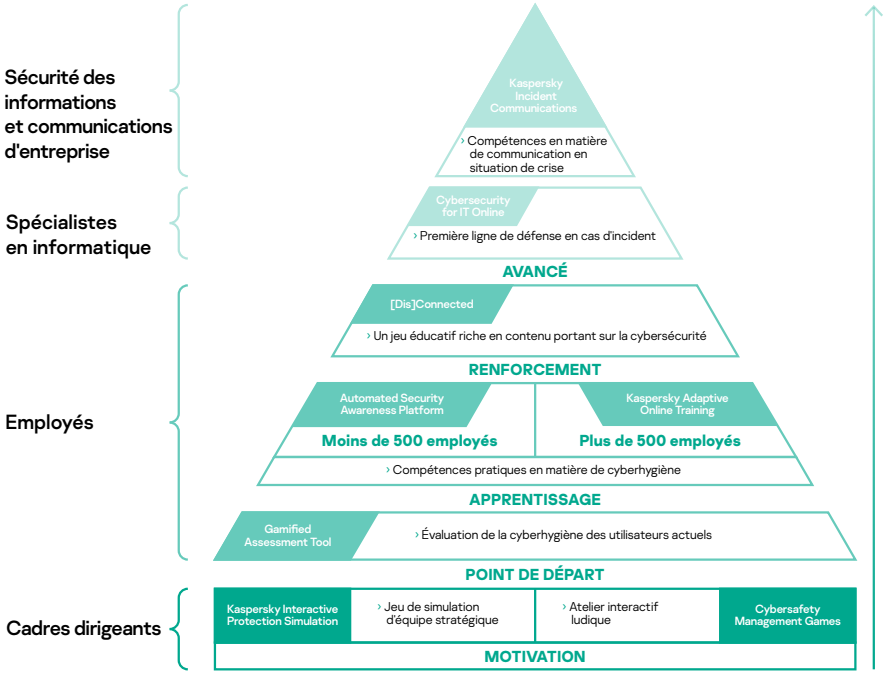
52 %
des entreprises
ont subi des incidents de cybersécurité causés par une mauvaise utilisation des ressources informatiques par les employés**

Plus de 1,7Mds$
de pertes financières
à cause de plaintes pour compromission d'emails professionnels***

Favoriser la motivation pour mieux sensibiliser à la sécurité

Votre plus grand défi en matière de cybersécurité est de changer le comportement de vos employés. Les gens ne cherchent généralement pas à acquérir des compétences et à changer leurs habitudes, ce qui explique pourquoi les efforts éducatifs se révèlent être plus qu'une simple formalité. Une formation efficace se compose de différents modules, tient compte des particularités de la nature humaine et de la capacité à assimiler les compétences acquises. Composé d'experts dans le domaine de la cybersécurité, Kaspersky connaît bien les comportements d'un utilisateur sensible à la cybersécurité. Grâce à nos connaissances et à notre expertise, nous avons ajouté des techniques et des méthodes d'apprentissage pour immuniser les employés de nos clients contre les attaques tout en leur donnant la liberté d'exceller sans limites.

Différents formats de formation pour différents niveaux organisationnels



* Rapport : « On the Money : Growing IT Security Budgets to Protect Digital Transformation Initiatives » (Viser juste : augmentation des budgets de sécurité informatique pour protéger les initiatives de transformation numérique). Kaspersky Lab, 2019

** Rapport : « IT security economics in 2019 », Kaspersky

*** FBI « 2019 Internet Crime Report » (Rapport du FBI sur la criminalité sur Internet)

Produits Kaspersky Security Awareness

Engagement/ Motivation

Point de départ

Apprentissage

Renforcement

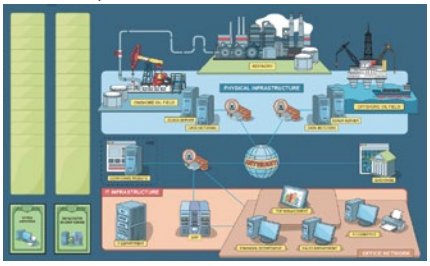
Motivation

Les employés ne sont pas toujours intéressés par une formation obligatoire plus poussée, et lorsqu'il s'agit de cybersécurité, nombreux sont ceux qui la jugent trop compliquée ou ennuyeuse, ou qui pensent qu'ils n'en ont pas besoin. Sans la motivation nécessaire pour apprendre, il est peu probable que le résultat de l'apprentissage soit très positif. Un autre défi pour les personnes chargées de l'éducation est d'impliquer les responsables d'entreprises dans la formation, même si leurs erreurs peuvent coûter à l'entreprise autant que celles des autres. C'est là qu'intervient le côté ludique. En effet, il s'agit du moyen le plus efficace d'encourager votre personnel à surmonter sa résistance initiale à la formation.

70 %
du contenu appris
est oublié au bout d'une journée avec les formes traditionnelles de formations

42 % des répondants travaillant dans des entreprises de plus de 1 000 employés ont déclaré que la majorité des programmes de formation qu'ils ont suivis étaient inutiles et inintéressants**

La formation KIPS s'adresse aux cadres supérieurs, aux experts en systèmes d'entreprise et aux professionnels de l'informatique, afin de les sensibiliser aux risques et aux défis liés à l'utilisation de toutes sortes de systèmes et de processus informatiques.



* « Courbe de l'oubli » de Ebbinghaus

** « The digital talent gap », Capgemini

Jeu stratégique Kaspersky Interactive Protection Simulation (KIPS) : la cybersécurité du point de vue des entreprises

KIPS est un jeu d'équipe interactif de 2 heures, qui établit la compréhension entre les décideurs (cadres supérieurs, responsables du service informatique et de la cybersécurité) et transforme leur perception de la cybersécurité. Il présente un logiciel de simulation de l'impact réel des programmes malveillants et des autres attaques sur les performances de l'entreprise et les recettes. Il oblige les joueurs à penser stratégiquement, à anticiper les conséquences d'une attaque et à réagir en conséquence dans les limites de temps et d'argent. Chaque décision a une incidence sur tous les processus commerciaux... l'objectif principal est de faire en sorte que les activités se déroulent correctement. L'équipe qui termine le jeu avec le plus de revenus, ayant trouvé et analysé tous les pièges du système de cybersécurité et y ayant répondu de manière appropriée, gagne.

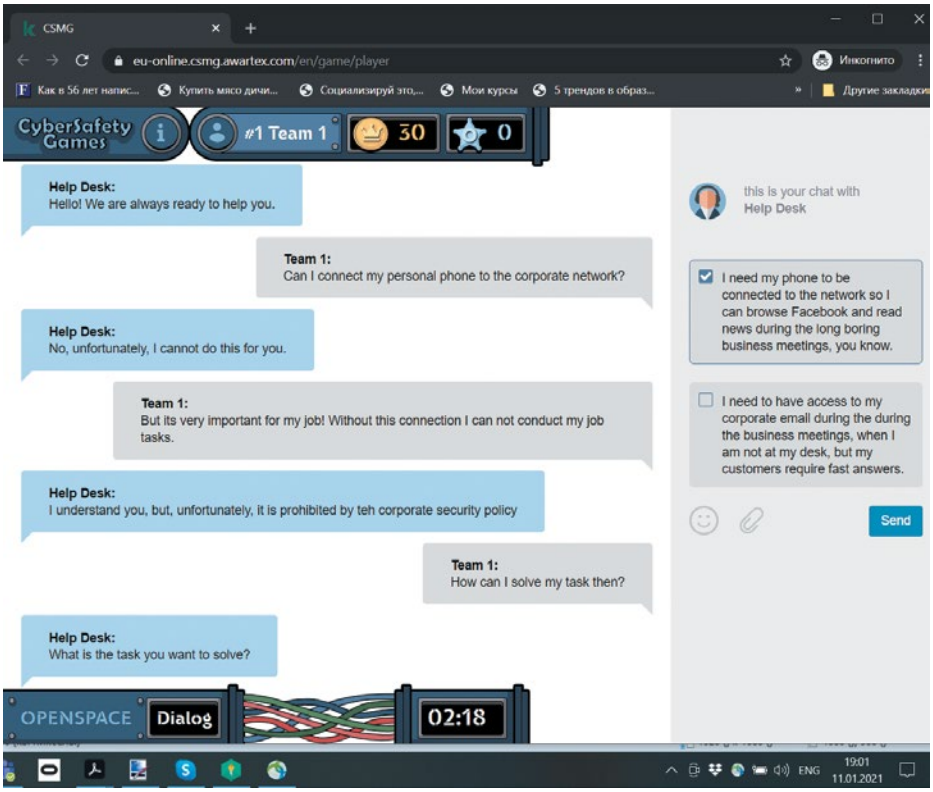
10 scénarios liés à l'industrie (d'autres s'ajoutent constamment)

Chaque scénario démontre le véritable rôle de la cybersécurité sur le plan de la continuité et de la rentabilité des activités, en mettant en évidence les nouveaux défis et les nouvelles menaces, ainsi que les erreurs classiques que commettent les organisations lorsqu'elles mettent en place leur cybersécurité. Il encourage également la coopération entre les équipes commerciales et de sécurité, ce qui contribue à maintenir des opérations stables et durables contre les cybermenaces.

Cybersafety Management Games : transformer les chefs d'entreprise et les supérieurs hiérarchiques en défenseurs proactifs de la cybersécurité

Cybersafety Management Games est un atelier interactif (combinaison d'activités sur ordinateur et d'activités dirigées par un instructeur ou entièrement en ligne) qui donne aux supérieurs hiérarchiques les compétences, les connaissances et les attitudes essentielles pour maintenir un environnement de travail sûr dans leurs divisions, sans sacrifier l'efficacité. Cette formation transforme les cadres moyens et supérieurs en partisans et défenseurs de la cybersécurité, faisant de la cybersécurité un élément clé de la prise de décision quotidienne.

Au cours de la formation, nous identifions les fausses idées les plus courantes et nous aidons les responsables à comprendre pourquoi les employés ont tendance à ignorer les règles et les principes de la cybersécurité. Grâce à des exercices spécialement conçus, nous démontrons ensuite comment transformer ces fausses idées en un comportement positif et sûr sur Internet.



Engagement/ Motivation

Point de départ

Apprentissage

Renforcement

Gamified Assessment Tool : un moyen rapide et passionnant d'évaluer les compétences des employés dans le domaine de la cybersécurité

L'outil Kaspersky Gamified Assessment Tool (GAT) vous permet d'estimer rapidement le niveau de connaissances de vos employés dans le domaine de la cybersécurité. L'approche intéressante et interactive élimine l'ennui que l'on trouve souvent dans les outils d'évaluation classiques. Il suffit aux employés de 15 minutes pour passer en revue 12 situations quotidiennes liées à la cybersécurité, évaluer si les actions du personnage sont risquées ou non et indiquer leur niveau de confiance dans leur réponse.

Après avoir terminé, les utilisateurs reçoivent un certificat avec un score qui reflète leur niveau de sensibilisation à la cybersécurité. Ils reçoivent également des commentaires pour chaque zone, accompagnés d'explications et de conseils utiles.

L'approche ludique de GAT motive les employés tout en leur présentant les éventuelles lacunes dans leurs connaissances lorsqu'ils résolvent certaines situations de cybersécurité. Cet outil est également utile pour les départements IT/RH, car il leur permet de mieux comprendre les niveaux de sensibilisation à la cybersécurité dans leur organisation et peut servir d'introduction à une campagne d'éducation plus large.

Point de départ

Les gens ne sont généralement pas conscients de leur niveau d'incompétence, ce qui les rend particulièrement vulnérables. Ils doivent être évalués, et recevoir des commentaires clairs et détaillés sur leur niveau de compétence en matière de cybersécurité pour que la poursuite de la formation soit efficace. Cela permet également de ne pas perdre de temps avec du matériel déjà connu.

Engagement/ Motivation

Point de départ

Apprentissage

Renforcement

Apprentissage

Nos plateformes d'apprentissage en ligne sont au cœur du programme de sensibilisation. Elles proposent **plus de 300 compétences en matière de cybersécurité** couvrant tous les grands thèmes de la sécurité informatique, y compris les mots de passe et les comptes, la sécurité des emails, les réseaux sociaux et les messageries, la sécurité des PC, le RGPD, etc.

Chaque leçon comprend des cas et des exemples réels afin que les employés puissent ressentir le lien avec ce qu'ils doivent affronter au quotidien dans le cadre de leur travail. Ensuite, ils peuvent appliquer ces compétences immédiatement après la première leçon.

Pour maximiser l'efficacité, nous utilisons des technologies adaptatives et construisons des parcours d'apprentissage automatisés pour chaque participant, en tenant compte de son niveau de connaissance initial et de son niveau cible (le niveau cible dépend du rôle que chaque participant joue dans l'entreprise). Il s'agit d'une démarche complexe, avec de nombreux exemples pratiques, beaucoup d'explications sur les raisons pour lesquelles elle est importante et de nombreuses évaluations qui fournissent des commentaires immédiats à propos des actions des utilisateurs.

« L'ignorance engendre plus souvent la confiance que la connaissance. »
Charles Darwin, La Filiation de l'homme

Sujets traités dans KAOT :
Mots de passe
- Sécurité de la messagerie électronique
- Navigation sur Internet
- Réseaux sociaux et messageries instantanées
- Protection PC
- Appareils mobiles
- RGPD

KAOT est actuellement proposé dans les langues suivantes : anglais, allemand, italien, français, espagnol, arabe et russe.

En savoir plus : kaspersky.com/kaot

Kaspersky Adaptive Online Training : la cybersécurité vue par un leader des solutions de sécurité informatique et associée à une méthodologie d'apprentissage adaptatif

Kaspersky Adaptive Online Training (KAOT) est une solution unique qui allie un contenu qui reflète plus de 20 ans d'expérience dans la cybersécurité et une méthodologie poussée d'apprentissage et de développement. KAOT est le fruit d'une collaboration entre Kaspersky et Area9 Lyceum, leader des systèmes d'apprentissage adaptatif.

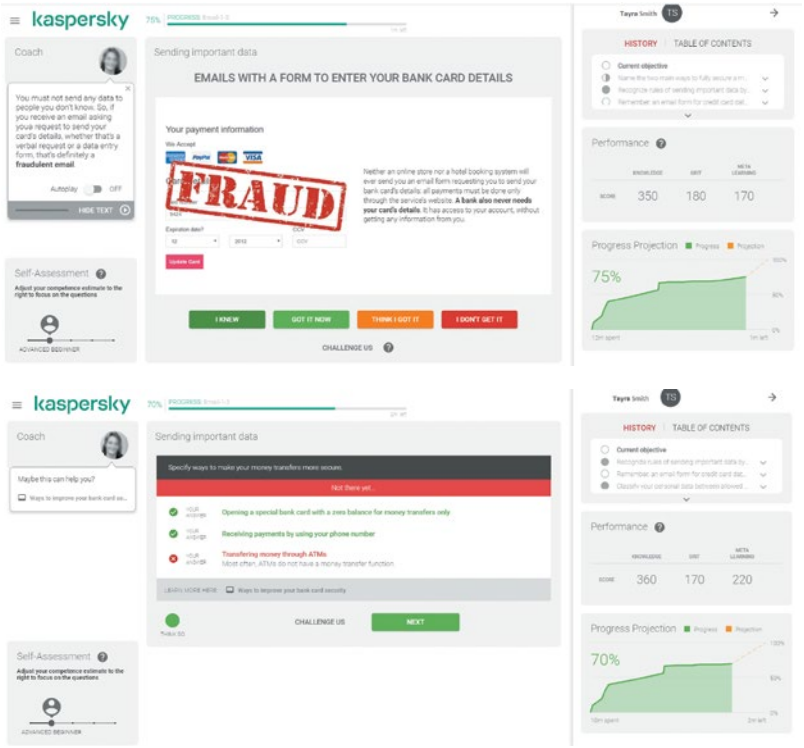
Fondée sur une méthodologie innovante d'apprentissage adaptatif, l'approche cognitive contribue à créer une expérience d'apprentissage personnalisée qui tient compte des capacités et des besoins propres à chaque participant.

Principaux avantages

- **L'approche de tuteur individuel** obtenue grâce à l'utilisation d'une méthodologie d'apprentissage adaptative.
- **La solution détecte les incompétences inconscientes et comble les lacunes,** motive l'apprentissage et assure durablement un comportement sûr. Le fait d'être conscient de ce que vous ne connaissez pas et de ce que vous devez améliorer vous permet de maîtriser la matière plus rapidement et plus efficacement.
- **La solution élimine l'ennui et la frustration** grâce à une approche personnalisée de chaque participant. Chaque leçon commence par une question suivie d'une leçon théorique uniquement lorsque cela est nécessaire. L'éducation centrée sur les problèmes renforce l'engagement et la participation à la cybersécurité.
- **La solution assure une utilisation automatique et systématique des compétences** grâce à des algorithmes adaptatifs qui permettent aux participants d'avancer en fonction de leurs compétences, en utilisant différentes approches du même sujet lorsque cela est nécessaire et en évaluant constamment le progrès de la personne. La formation comble les lacunes de compétences et permet d'acquérir rapidement et efficacement de nouvelles compétences. À un niveau de compétence élevé, certaines connaissances deviennent une seconde nature, de sorte que les actions deviennent automatiques et habituelles, constamment renforcées par des activités de « rafraîchissement » lorsqu'un participant risque d'oublier le contenu.

Suivi des résultats

De nombreuses données statistiques vous permettent de suivre les progrès des employés : synthèse des performances, rapports et schémas individuels et de groupe. L'administrateur peut identifier ceux qui ont les meilleurs résultats et ceux qui ont besoin d'une aide supplémentaire. Il peut également consulter les rapports relatifs aux progrès des utilisateurs, aux progrès des classes et aux détails des attributions avec une analyse approfondie des compétences des employés et de la métacognition.



Kaspersky Automated Security Awareness Platform : un outil en ligne facile à gérer qui permet aux employés de développer leurs compétences dans le domaine de la cybersécurité, niveau par niveau

Kaspersky ASAP est un outil en ligne efficace et facile à utiliser qui façonne les compétences des employés dans le domaine de la cybersécurité et les motive à adopter le bon comportement.

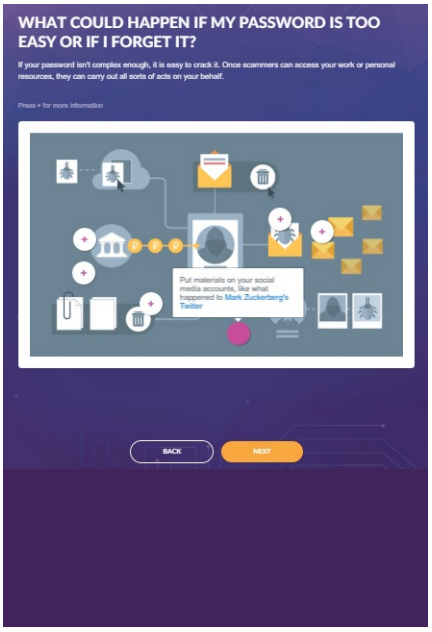
Cette formation est idéale pour les petites et moyennes entreprises, en particulier celles qui ne disposent pas de ressources dédiées à la gestion des programmes de formation.

Principaux avantages :

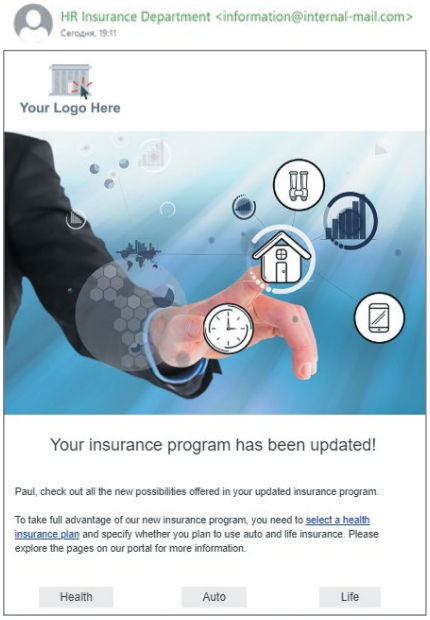
- **Simplicité grâce à une automatisation complète :** le programme est très facile à lancer, configurer et surveiller, et la gestion en continu est entièrement automatisée. Aucune intervention administrative n'est requise. La plateforme génère un programme de formation pour chaque groupe d'employés, en offrant un apprentissage par intervalles, fourni automatiquement par l'intermédiaire de différents formats de formation, comme des modules d'apprentissage, du renforcement par email, des tests ou des simulations d'attaques de phishing.
- **Efficacité :** le contenu du programme est structuré de façon à favoriser un apprentissage incrémentiel par intervalles avec un renforcement constant. La méthodologie est basée sur les particularités de la mémoire humaine, afin d'assurer la conservation des connaissances et l'application ultérieure des compétences acquises.
- **Options de licensing flexible** (pour les fournisseurs de services managés) : le modèle de licensing par utilisateur démarre à partir de 5 licences seulement.

Chaque thème comprend différents niveaux, chacun contribuant à développer des compétences spécifiques en matière de sécurité. Les niveaux sont définis selon le degré de risque qu'ils visent à éliminer. Le niveau 1 concerne le comportement à adopter face à des attaques directes et massives. Les niveaux plus élevés offrent une formation de sensibilisation aux attaques plus sophistiquées et ciblées.

Leçons interactives



Simulations d'attaques de phishing



Suivi des résultats

Vous pouvez suivre la progression des employés à partir du tableau de bord et évaluer la progression de toute l'entreprise, et de tous les groupes, en un coup d'œil. Il est également possible d'accéder à plus de détails de façon individuelle.

Un parcours d'apprentissage automatisé pour lutter contre l'oblitération et assurer la rétention des compétences

Sujets traités dans ASAP :
Mots de passe et comptes
- Sécurité de la messagerie électronique
- Navigation sur Internet
- Réseaux sociaux et messageries instantanées
- Protection PC
- Appareils mobiles
- Protection des données confidentielles
- RGPD

Kaspersky ASAP est une solution multilingue, actuellement proposée en anglais, en allemand, en italien, en français, en espagnol, en russe, en arabe, en portugais, en néerlandais, en tchèque, en polonais, en kazakh, en slovène, en roumain, en turc et en hongrois*.

ASAP est une solution idéale pour les MSP et xSP : les services de formation de plusieurs entreprises peuvent être gérés par le biais d'un compte unique, et les licences peuvent être achetées via un abonnement mensuel.

Bénéficiez d'une version d'essai entièrement fonctionnelle de Kaspersky ASAP sur asap.kaspersky.fr : vous constaterez par vous-même à quel point il est simple de configurer et de gérer votre propre programme de formation et de sensibilisation à la cybersécurité en entreprise.

Engagement/ Motivation

Point de départ

Apprentissage

Apprentissage avancé

Renforcement

Avancé

La plupart des entreprises proposent une formation à la cybersécurité sur deux niveaux : une formation d'experts pour les équipes de sécurité informatique et une formation de sensibilisation à la sécurité pour les employés ne travaillant pas dans les services informatiques (Kaspersky offre un ensemble complet de produits pour les deux). Cependant, quelles catégories d'employés nous échappent ? Les équipes informatiques, les équipes de support technique et les autres employés ayant un niveau avancé d'un point de vue technique. Les programmes de sensibilisation standard ne leur suffisent pas, mais les entreprises n'ont pas besoin d'en faire des experts de la cybersécurité : ce n'est pas nécessaire, et cela coûte trop cher et prend trop de temps.

La formation CITO est menée 100 % en ligne : les participants devront seulement disposer d'une connexion Internet ou d'un accès au système LMS de leur entreprise et du navigateur Chrome.

Chacun des 4 modules comporte une brève présentation théorique, des conseils pratiques et entre 4 et 10 exercices. Ces exercices permettent de mettre en pratique certaines compétences et d'apprendre à utiliser les logiciels et les outils de sécurité informatique dans son travail au quotidien.

L'entraînement KIC assure que votre équipe de crise :

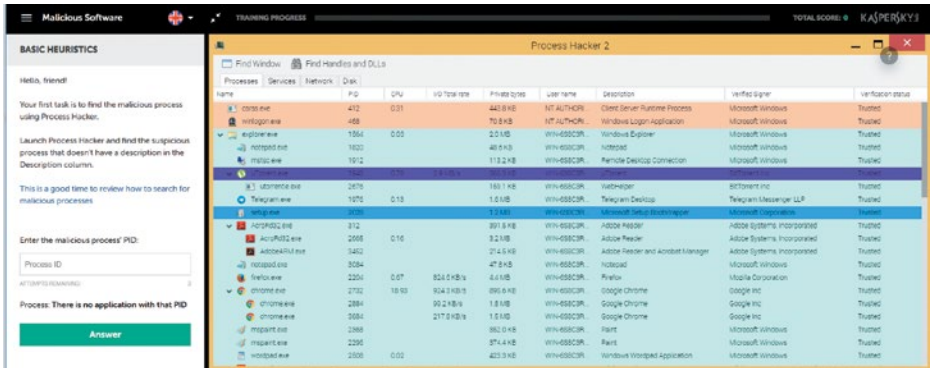
- Comprend les cybermenaces auxquelles vous êtes exposés
- Reconnaît les conséquences potentielles
- Peut assurer une coordination efficace avec votre équipe de sécurité informatique
- Acquiert de l'expérience grâce à une simulation de cyberincidents
- Sait ce qu'il est essentiel et sûr de dire dans le cadre de communications internes et externes à la suite d'une cyberattaque
- Actualise et met en œuvre votre plan de communication en cas de cybercrise

Cybersecurity for IT Online : la première ligne de défense contre les incidents

Cybersecurity for IT Online est une formation interactive destinée à tous ceux qui travaillent dans le domaine de l'informatique. Elle développe de solides compétences en matière de cybersécurité et de réponse aux incidents de premier niveau.

Le programme fournit aux professionnels de l'informatique des compétences pratiques sur la façon de reconnaître une attaque possible au cours d'un incident PC qui semble inoffensif. Il leur apprend également à recueillir des données sur les incidents pour les transmettre à la sécurité informatique. Ce programme rend la traque des symptômes de présence d'un logiciel malveillant intéressante et renforce ainsi le rôle de tous les membres de l'équipe informatique en tant que première ligne de défense du point de vue de la sécurité. Il se compose de quatre modules : les logiciels malveillants, les programmes et les fichiers potentiellement indésirables, les bases en matière d'enquête et la réponse aux incidents de phishing.

Cette formation est recommandée pour tous les spécialistes en informatique au sein de votre entreprise, à commencer par les équipes de support technique et les administrateurs système. La plupart des membres non experts de l'équipe de sécurité informatique bénéficieront également de cette formation.



Kaspersky Incident Communications : donner les moyens à l'équipe de communication de votre entreprise de répondre à une cyberattaque

Dès l'instant où un cyberincident est découvert, chaque action compte. La façon dont vos communications sont gérées, en externe et en interne, est essentielle, en particulier lorsqu'il s'agit de traiter des vecteurs d'attaque inconnus et des menaces persistantes avancées (APT).

Kaspersky Incident Communications forme les cadres supérieurs, et les professionnels de la sécurité des informations et de la communication d'entreprise sur les façons de gérer les communications de crise, y compris la mise en place et l'utilisation des moyens appropriés. Cette solution permet d'établir des liens solides entre les membres d'une équipe de crise et explique comment préparer un plan de communication de crise. Elle fournit des recommandations pratiques, des procédures de sécurité des opérations et des outils pour chiffrer les communications lors d'un cyberincident afin de favoriser la continuité des activités.

Engagement/ Motivation

Point de départ

Apprentissage

Renforcement

Renforcement

Le renforcement est une partie essentielle du programme d'apprentissage, et il est nécessaire pour consolider les connaissances et les compétences acquises pendant l'étape d'apprentissage.

La meilleure façon de transformer les compétences acquises en habitudes est de les mettre en pratique. En même temps, les gens commettent parfois des erreurs et apprennent de leur expérience personnelle. Cependant, lorsqu'il s'agit de cybersécurité, il peut être extrêmement coûteux de tirer les leçons de ses propres erreurs.

Grâce à une formation ludique, vous pouvez « vivre » une situation et en connaître les conséquences sans nuire, ni à a vous ni à votre entreprise.

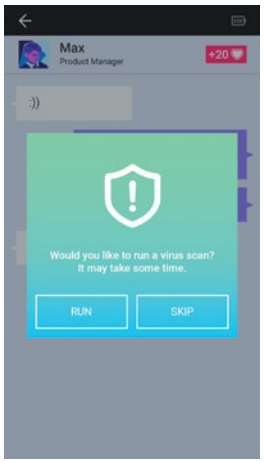
[Dis]connected : un jeu éducatif amusant

[Dis]Connected est un jeu de cybersécurité très immersif, présenté sous la forme d'un roman visuel, où les utilisateurs sont mis au défi de maintenir un équilibre sain entre leur vie professionnelle et leur vie privée, et de réussir tant sur le plan personnel que professionnel.

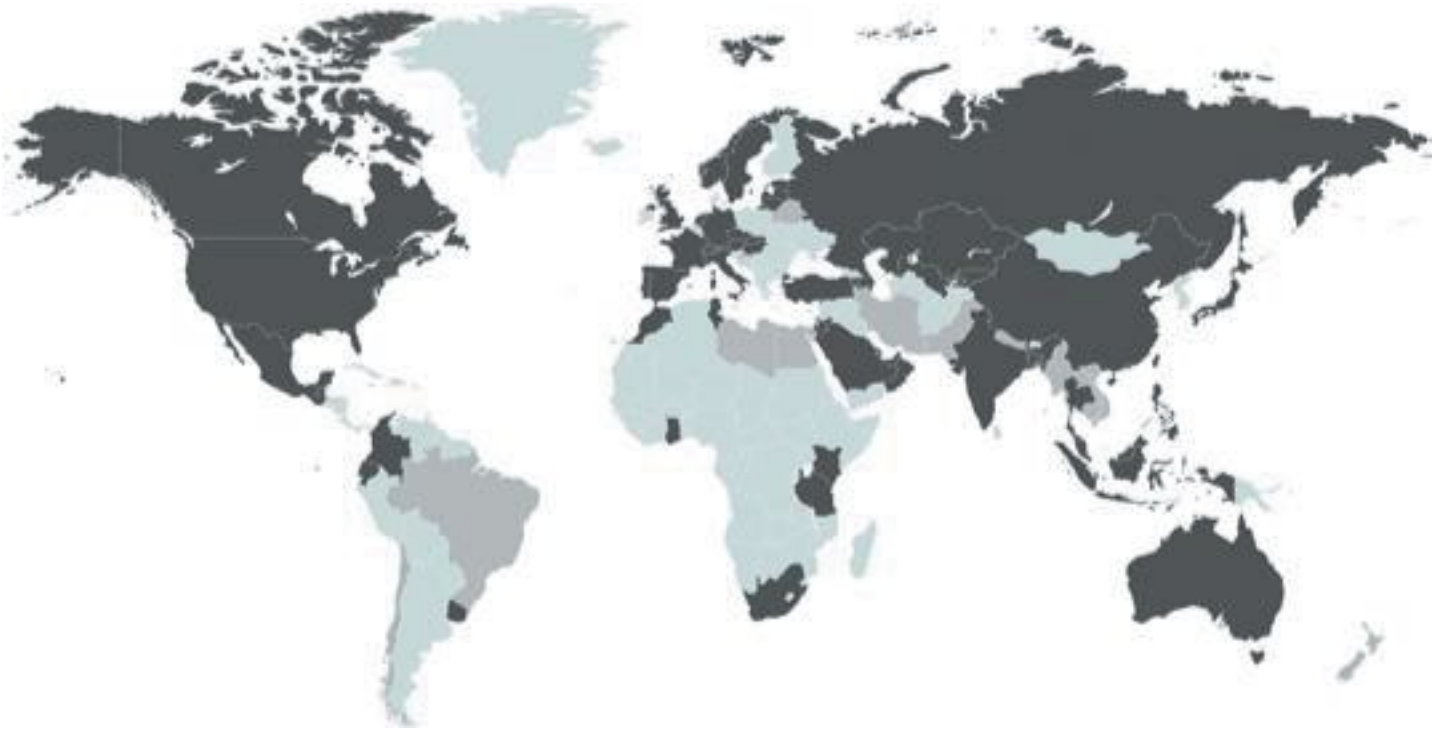
Des éléments de cybersécurité sont intégrés dans l'intrigue du jeu, et celui-ci révèle comment nos décisions en matière de cybersécurité peuvent contribuer à atteindre (ou non) les objectifs. En tout, 18 situations doivent être résolues, notamment dans les domaines des mots de passe et des comptes, des emails, de la navigation sur le Web, des réseaux sociaux et des messageries, de la sécurité informatique et des appareils mobiles.

Des applications intégrées émulées (messageries, applications bancaires, etc.) assurent une expérience immersive encore plus complète.

À la fin du jeu, les joueurs reçoivent un compte-rendu de leur taux de réussite du projet et découvrent si leurs compétences en matière de sécurité sont suffisantes pour aujourd'hui, et pour demain.



Kaspersky Security Awareness dans le monde



75
pays

Plus de 500 000
employés formés

Kaspersky Security Awareness :
kaspersky.com/awareness
Actualités dédiées à la sécurité informatique :
business.kaspersky.com/

www.kaspersky.fr

kaspersky BIENVENUE DANS LE FUTUR