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

Kaspersky Security Awareness

kaspersky PRÊTS POUR L'AVENIR

Plus d'informations sur
https://www.kaspersky.fr/enterprise-security/security-awareness

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 membres de la direction déclarent que les employés constituent la plus grande menace pour la sécurité opérationnelle*

43 % des petites entreprises ont subi un incident de sécurité à la suite d'une violation des politiques de sécurité informatique par des employés**

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 des données de l'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.

* Rapport « Weathering the Perfect Storm: Securing the Cyber-Physical Systems of Critical Infrastructure », 2020

** Rapport « IT security economics 2021 » (Rapport sur la sécurité informatique en 2021), Kaspersky.

*** « 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…

1 315 000 $
par entreprise
Impact financier moyen des violations de données causées par une mauvaise utilisation des ressources informatiques par les employés*

50 %
des grandes entreprises
ont déclaré avoir été confrontées à des menaces directement causées par un comportement inapproprié du personnel, ce qui en fait la menace la plus courante pour la sécurité informatique*

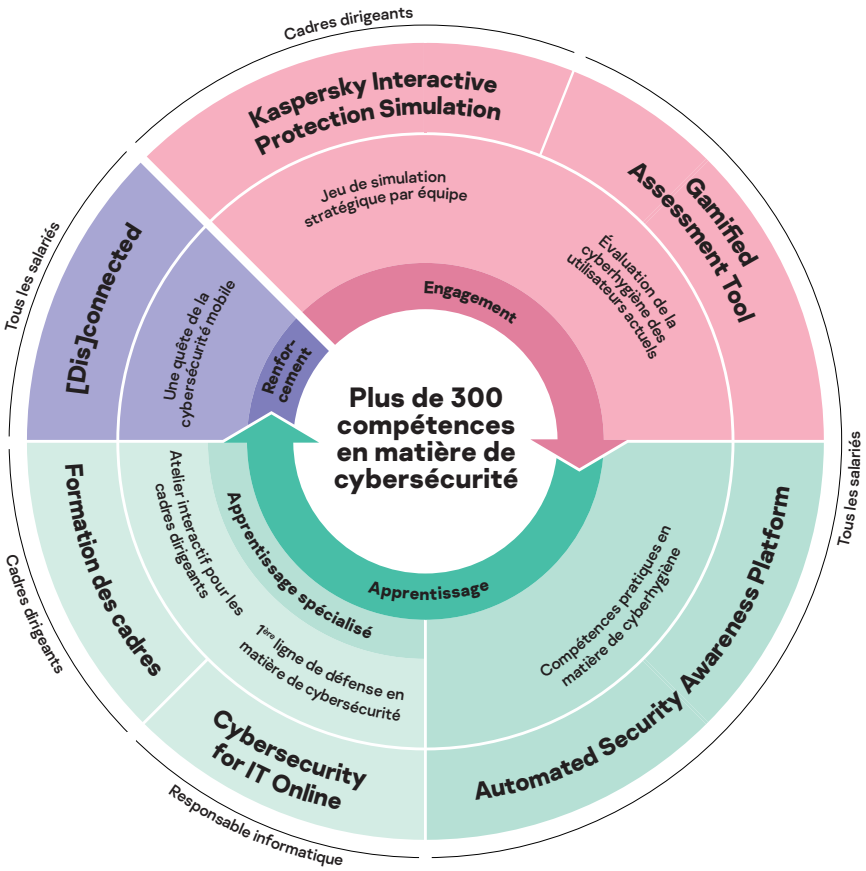
86 %
des entreprises
ont déclaré qu'au moins une personne avait cliqué sur un lien de phishing**

5,01 M $
le coût moyen par violation
des attaques BEC (BEC, ou compromission d'emails professionnels, est un type d'attaque de phishing où les attaquants détournent ou usurpent des comptes de messagerie d'entreprises légitimes)

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 « IT security economics 2021 » (Rapport sur la sécurité informatique en 2021), Kaspersky

** Tendances des menaces de cybersécurité en 2021, CISCO

*** Coût d'une violation de données, 2021. IBM

Solutions Kaspersky Security Awareness

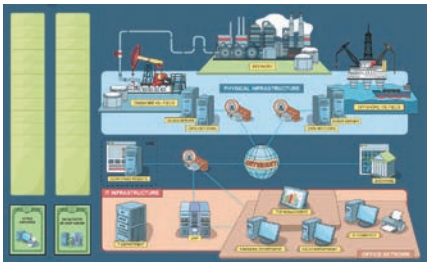
Motivation

Les salariés ne sont pas toujours intéressés par une formation obligatoire 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.



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.

13 scénarios liés à l'industrie
(d'autres s'ajoutent tout le temps)

Chaque scénario démontre le 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.

Personnalisation des scénarios

À partir du troisième trimestre 2022, pour certains scénarios industriels, les entreprises pourront créer leurs propres scénarios de jeu avec différentes attaques. En utilisant différentes combinaisons d'attaques, les entreprises disposant d'une licence KIPS pour les entreprises peuvent jouer plusieurs fois le même scénario industriel.

KIPS Virtual Reality

KIPS Power Station VR est une nouvelle expérience immersive dans un environnement réaliste aussi proche que possible des opérations réelles d'une centrale électrique. La technologie permet aux managers de « travailler » en tant que spécialistes de la sécurité informatique, en démontrant visuellement le rôle de la cybersécurité et son impact sur les entreprises, afin qu'ils puissent constater les conséquences de leurs décisions informatiques dans des représentations 3D très réalistes, au lieu de n'en avoir qu'une idée abstraite.

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.

Apprentissage

Notre plateforme d'apprentissage en ligne est au cœur du programme de sensibilisation. Elle contient **plus de 300 compétences en matière de cybersécurité** couvrant tous les grands thèmes de la sécurité informatique. Chaque leçon comprend des cas et des exemples réels afin que les employés puissent faire 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.

Kaspersky ASAP : un outil en ligne facile à gérer qui renforce, niveau par niveau, les compétences de vos employés en matière de cybersécurité

Sujets traités dans ASAP :

- Mots de passe et comptes
- Email
- Sites Web et Internet
- Réseaux sociaux et messageries
- Sécurité pour PC
- Appareils mobiles
- Protection des données confidentielles
- RGPD
- Cybersécurité industrielle

Formation express ASAP

Une version courte de la formation au format audiovisuel.

- Théorie interactive
- Vidéos
- Tests

Kaspersky ASAP est une solution multilingue.

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.

Kaspersky Automated Security Awareness Platform : efficacité et facilité de gestion des formations pour les organisations de toute taille

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.

Bien que la formation réponde aux besoins de sensibilisation à la sécurité de toutes les entreprises, la gestion automatisée intéressera particulièrement celles qui ne disposent d'aucune ressource dédiée à la gestion des formations.

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.
- **Apprentissage flexible :** choisissez le type de formation qui convient le mieux à vos besoins, qu'il s'agisse d'attribuer aux employés une formation express de base qui vous aidera à répondre rapidement aux exigences réglementaires en matière de formation à la cybersécurité ou à actualiser leurs connaissances, ou de choisir une formation principale répartie en niveaux de complexité pour développer des compétences plus détaillées et plus approfondies en matière de cybersécurité.
- **Options de licensing flexible** (pour les fournisseurs de services managés) : le modèle de licensing par utilisateur démarre à partir de 5 licences seulement.

ASAP est idéale pour les MSPs et les xSP : les services de formation pour plusieurs entreprises peuvent être gérés par un seul compte, et des abonnements mensuels à des licences sont disponibles.

Essayez une version complète de Kaspersky ASAP à l'adresse https://asap.kaspersky.com/fr/. Constatez par vous-même à quel point il est facile de mettre en place et de gérer votre propre programme de de sensibilisation à la sécurité d'entreprise !

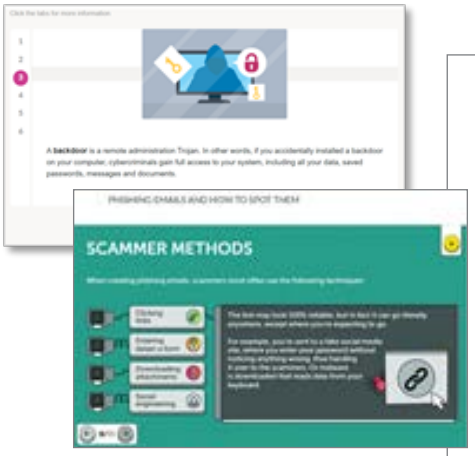
Simulations de campagnes de phishing

Des attaques de phishing simulées peuvent être utilisées avant, pendant et après la formation, afin de tester la faculté des employés à résister aux cyberattaques et de les aider, eux et la direction de l'entreprise, à constater les avantages de la formation.

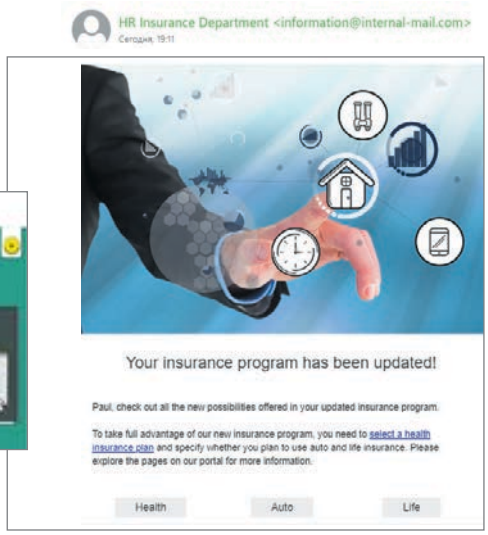
Formation principale

Formation express

Leçons interactives



Simulations d'attaques de phishing



Suivi des résultats

Vous pouvez suivre la progression de vos salariés à partir du tableau de bord et évaluer la progression de toute l'entreprise, et de tous les groupes, en un coup d'œil. Vous pouvez également accéder à des informations plus détaillées à un niveau individuel.

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 parcours de cybersécurité mobile

[Dis]connected est un jeu de cybersécurité mobile 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) ces 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 totalement immersive.

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.

Le jeu fonctionne sur les téléphones mobiles. Une **démo gratuite** est disponible dans Google Play et dans l'AppStore : **https://kas.pr/mobilestores**

Apprentissage avancé

Spécialistes généraux en informatique : les services d'assistance et les autres membres du personnel disposant de connaissances techniques sont souvent exclus de la formation parce que les programmes de sensibilisation standard ne leur suffisent pas, mais les entreprises n'ont pas non plus besoin d'en faire des experts en cybersécurité : c'est trop coûteux, trop long et inutile.

Nous sommes ravis d'annoncer une formation qui comble cette lacune – pas aussi approfondie qu'une formation d'expert, mais plus avancée qu'une formation destinée aux autres salariés.

Modules de formation CITO :

- Logiciels malveillants
- Programmes et fichiers potentiellement indésirables
- Notions de base sur les enquêtes
- Gestion des incidents de phishing
- Sécurité du serveur
- Sécurité d'Active Directory

Méthode de diffusion de la formation CITO :
Format Cloud ou SCORM

Essayez gratuitement l'un des modules CITO : cito-training.com

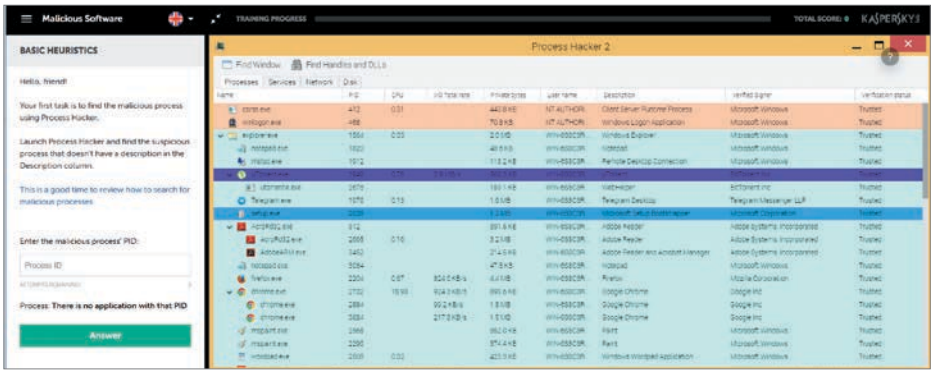
Cybersecurity for IT Online : la première ligne de défense contre les incidents

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.

Ce programme permet aux professionnels de l'informatique d'acquérir des compétences pratiques pour reconnaître un scénario d'attaque possible lors d'un incident informatique à première vue bénin. 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.

La formation CITO enseigne également les principes d'investigation fondamentaux et apprend à utiliser les outils et logiciels de sécurité informatique, en plus de développer des compétences théoriques, pratiques et basées sur des exercices qui permettront à vos professionnels informatiques de collecter les données sur les incidents en vue d'un transfert vers l'équipe de sécurité informatique.

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.



Les cadres supérieurs font partie des cibles les plus recherchées par les cybercriminels, mais ils représentent souvent un véritable défi pour les formateurs. Toutefois, sans leur participation et sans leur soutien aux diverses initiatives et actions de défense en matière de cybersécurité, il est impossible de créer une culture de la cybersécurité au sein d'une organisation.

La cybersécurité est un aspect important de la génération de revenus, au même titre que la gestion de projet, les instruments financiers et l'efficacité opérationnelle des entreprises. Voilà l'objet de notre cours destiné aux dirigeants.

Formation des cadres : renforcement de la résilience des entreprises dans le cadre de la transformation numérique

Les chefs d'entreprise et les cadres supérieurs apprennent les bases de la cybersécurité grâce à une formation encadrée par un tuteur qui leur permet de mieux comprendre les cybermenaces et la façon de s'en protéger.

Les recherches révèlent qu'il existe un lien direct entre la rapidité et l'efficacité de la réponse aux incidents et l'ampleur des dommages qu'un incident peut causer. La formation accorde une attention particulière aux aspects financiers de la cybersécurité et à la faisabilité des investissements dans ce domaine, ce qui permet aux membres de la direction de mieux comprendre le lien entre la cybersécurité et les performances de l'entreprise.

La simulation Kaspersky Interactive Protection (KIPS) peut être utilisée en complément de cette formation pour consolider davantage les acquis par des exercices pratiques.

Objectifs de la formation

- Partager les dernières informations concernant les cybermenaces modernes et leurs risques pour les entreprises
- Informer les participants de l'état actuel des cybermenaces
- Permettre de mettre en pratique les règles de base de la culture de cybersécurité à la fois sur le plan personnel et professionnel
- S'assurer que l'impact sur les activités des principales questions réglementaires dans le domaine de la sécurité informatique a bien été compris
- Clarifier les concepts de base en matière de cybersécurité ainsi que les méthodes de protection contre les attaques ciblées
- Proposer des recommandations pratiques concernant la politique de l'entreprise
- Fournir des conseils en matière de communication pour répondre aux incidents et enquêter sur ceux-ci

Kaspersky Security Awareness : une formation flexible

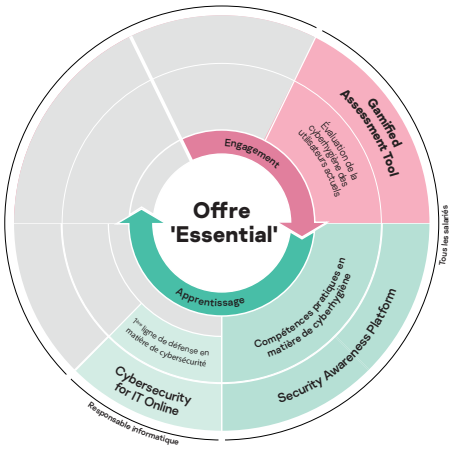
Les solutions de formation de Kaspersky couvrent tous les départements de votre entreprise et peuvent être utilisées seules ou collectivement. Nous facilitons également la prise en main grâce à des formules adaptées à vos besoins.

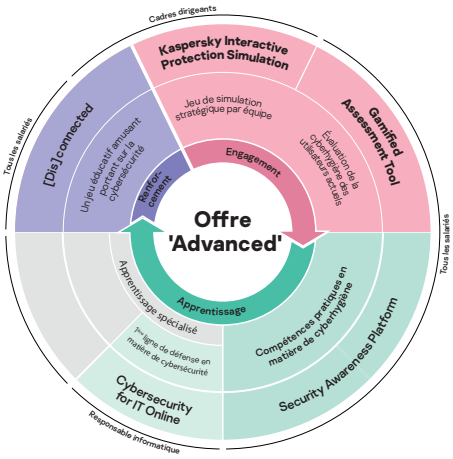
L'option qui sensibilise vos collaborateurs à la cybersécurité en toute simplicité : simple à mettre en place, simple à gérer.

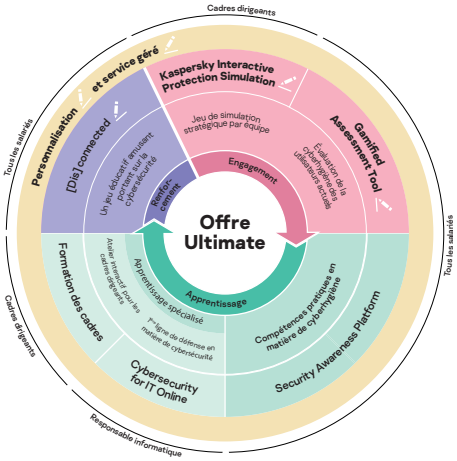
Fournit un niveau de base de formation à la sécurité pour vous aider à assurer le bon fonctionnement de vos activités et à répondre aux exigences réglementaires ou à celles des tiers en matière de formation générale à la cybersécurité

Aide les grandes entreprises à assurer la continuité de leur activités au moyen d'une solution de formation simple et clé en main. S'adresse à tous les niveaux de l'entreprise et modifie les comportements en couvrant toutes les étapes du cycle d'apprentissage.

Assure une sensibilisation maximale à la cybersécurité, avec une personnalisation et des services gérés, afin que les cadres dirigeants soient préparés grâce à une parfaite maîtrise des scénarios de menaces, que les employés disposent de compétences systématiques en matière de cybersécurité et que le personnel informatique généraliste vous aide en tant que première ligne de défense.







La formation Kaspersky Security Awareness utilise les dernières méthodes de formation et des techniques avancées pour assurer un bon résultat. De nouvelles solutions prêtes à l'emploi et flexibles peuvent être adaptées à vos besoins. Il existe donc une solution pour tout le monde. Pour en savoir plus, rendez-vous sur kaspersky.fr/awareness

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

kaspersky.fr

kaspersky PRÊTS POUR L'AVENIR