Kaspersky
Security
Awareness

Concevoir une culture de cybersécurité qui assure la sécurité de votre entreprise

kaspersky cybersecurity
true to business

Erreur humaine

menace majeure : en moyenne, 64 à 86 % des violations de données sont dues à des actions humaines non malveillantes[1]

$ 4,4 millions

coût moyen d'une violation des données par organisation[2]

La réglementation impose une sensibilisation à la sécurité

dans le cadre de la mise en conformité : les normes PCI DSS, ISO/IEC 27001, RGPD, NIS 2 et d'autres exigent ou recommandent vivement la mise en place de programmes de sensibilisation à la sécurité afin de protéger les données sensibles

Cultiver une culture soucieuse de la sécurité porte ses fruits

Une étude de Kaspersky montre que plus de 85 % des employés ayant suivi une formation de sensibilisation font état d'une vigilance et d'une prudence accrues – un changement de comportement qui contribue à prévenir les incidents.

92 %

des utilisateurs recommanderaient Kaspersky Security Awareness

3 millions

d'employés ont été formés par nos programmes de formation

Plus de 160

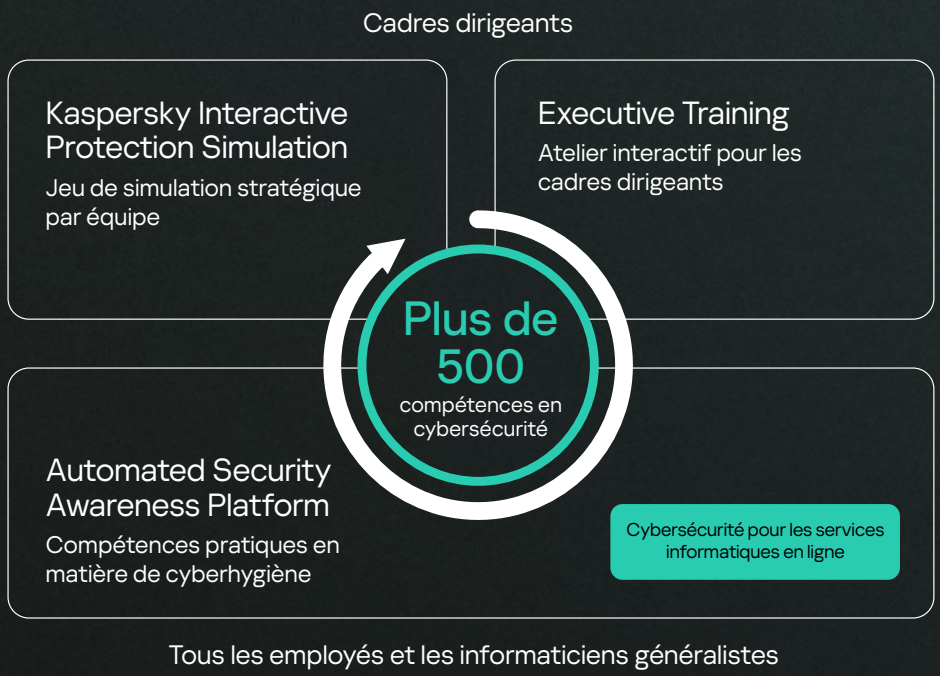
pays où des entreprises protègent leurs employés grâce à nos solutions de formation

Une approche efficace pour réduire le cyberrisque humain

Développez une cyberculture au sein de votre organisation, fondée sur une forte sensibilisation à la cybersécurité et des compétences pratiques. Vous contribuerez ainsi à réduire le nombre d'incidents causés par l'erreur humaine. La meilleure façon de traiter le facteur humain est de mettre en place un programme de formation structuré, combinant des contenus pertinents et à jour avec les méthodes et technologies d'apprentissage les plus récentes.

Solutions Kaspersky Security Awareness

Kaspersky Security Awareness permet aux entreprises de toutes tailles à travers le monde d'améliorer les connaissances de leurs employés en matière de cybersécurité et de promouvoir une culture où la sécurité incombe à chacun. Comme les changements de comportement durables prennent du temps, notre approche consiste à mettre en place un cycle d'apprentissage continu à l'aide de divers outils et supports pédagogiques : Kaspersky Interactive Protection Simulation, Executive Training, Automated Security Awareness Platform et Cybersecurity for IT Online.



Pourquoi les clients choisissent Kaspersky Security Awareness

Les compétences et la confiance nécessaires pour détecter les menaces réelles et y faire face

En nous appuyant sur près de 30 ans d'expertise de Kaspersky en matière de cybersécurité et sur notre Threat Intelligence en temps réel, nous élaborons des contenus de formation en cybersécurité très pertinents. À mesure que de nouvelles menaces apparaissent, notre contenu évolue, ce qui permet de garantir que vos employés sont toujours bien préparés.

Un changement de comportement durable

Notre méthodologie permet de consolider les nouvelles compétences, d'assurer une motivation constante et d'intégrer l'apprentissage aux routines organisationnelles. Il en résulte un changement durable des comportements, où les pratiques sécuritaires deviennent une seconde nature.

Un apprentissage accessible et interactif

Nos formations reposent sur un apprentissage interactif avec une structure claire et logique qui aide les employés à faire le lien entre les cours et leurs tâches quotidiennes, ce qui améliore la compréhension, la mémorisation et la mise en pratique.

Une mobilisation à tous les niveaux

Que ce soit pour les cadres supérieurs à la recherche d'informations stratégiques et exploitables ou pour l'équipe de terrain ayant besoin de conseils concrets, nous fournissons le contenu adapté, dans le format approprié, à chaque public.

1 Rapport Kaspersky Human Factor 360, Cybersecurity Ventures, rapports sur les violations des données de Verizon
2 Rapport sur le coût d'une violation de données en 2025, IBM

Kaspersky Automated Security Awareness Platform : construire un pare-feu humain

Kaspersky Automated Security Awareness Platform (ASAP) est un outil en ligne qui propose une formation continue, permettant ainsi aux employés d'acquérir les compétences et les connaissances nécessaires pour identifier et contrer les vecteurs d'attaque réels.

Développé par des experts de renommée mondiale, Kaspersky ASAP donne les moyens à vos collaborateurs d'agir et renforce votre entreprise :

Réduit le nombre d'incidents liés au facteur humain ainsi que les préjudices financiers et les atteintes à la réputation qui en découlent

Réduit le risque de sanctions pour non-conformité en facilitant le respect des exigences réglementaires

Réduit le temps et les efforts nécessaires à la gestion des formations de sensibilisation et allège la charge de travail des équipes informatiques

Kaspersky ASAP est bien plus qu'un simple outil anti-phishing. La formation s'appuie sur les techniques du modèle MITRE ATT&CK, en indiquant les vecteurs d'attaque d'origine humaine que les employés peuvent aider à prévenir. Exemples :

Technique MITRE	Menace	Compétences et comportements visés
T1566 : Phishing	E-mails malveillants	Identifier et signaler les tentatives de phishing
T1585 : Créer des comptes	Faux comptes/profils	Vérifier l'authenticité avant de partager des informations
T1199 : Relation de confiance	Abus de confiance de partenaires	Apprendre à remettre en question les demandes inhabituelles
T1091 : Réplication via un support amovible	Supports amovibles	Comprendre les risques liés aux programmes malveillants sur les clés USB
T1078 : Comptes valides	Vol de données d'identification	Éviter de donner accès par le biais de techniques d'ingénierie sociale

95 %

des employés formés sont désormais capables de repérer les attaques de phishing

20x

moins de violations de données lorsque les employés sont formés régulièrement[1]

Voici quelques-uns des principaux thèmes abordés dans ASAP :

- Email
- Mots de passe et comptes
- Sites et Internet
- Protection PC
- RGPD
- Données confidentielles
- Données personnelles
- Sécurité physique des données
- Intelligence artificielle et réseaux neuronaux
- Attaques contre des cadres supérieurs
- Périphériques mobiles,
- Réseaux sociaux et messageries
- Vishing
- Attaques contre les chaînes d'approvisionnement
- Cybersécurité industrielle
- Sécurité des cartes bancaires et norme PCI DSS
- Comment réagir en cas d'incident

Renforcez les compétences de vos employés afin qu'ils constituent un rempart supplémentaire aux côtés des outils techniques.

Commencer la période d'essai

1 2025 Kaspersky Automated Security Awareness Platform Research

Un contenu et une méthodologie qui marquent durablement, pour retenir les connaissances et appliquer les compétences

Piloté par des experts

Un contenu s'appuyant sur près de 30 ans d'expertise en cybersécurité et sur un modèle de compétences couvrant les connaissances pratiques et essentielles en matière de cybersécurité dans de nombreux domaines.

Contenu varié

Favorise la mémorisation des informations grâce à des modules et des exercices interactifs, des cas concrets, des tests, des vidéos et des simulations de phishing multiscénarios.

Large éventail d'options de personnalisation

Ajoutez votre logo et vos certificats de marque, agrémentez vos cours de diapositives internes, de documents ou de stratégies, ajoutez des modules SCORM/PDF personnalisés et adaptez la structure des tests.

Centré sur la nature humaine

Pensé pour s'adapter à la manière dont on assimile, mémorise et met en pratique les informations

Comment ça fonctionne ?

Chaque membre de votre organisation a besoin d'être sensibilisé à la cybersécurité, mais le niveau de connaissance requis varie en fonction du poste et du profil de risque. C'est là que les formations universelles échouent. Notre plateforme aide votre équipe à acquérir plus de 500 compétences pratiques, à regrouper facilement les collaborateurs et à attribuer la formation adaptée à chaque participant en quelques clics seulement, grâce aux modules ci-dessous.

Formation principale

Approfondissez vos connaissances grâce à de courtes leçons classées par niveau de complexité.

Formation express

Répondez rapidement aux exigences réglementaires en matière de formation à la cybersécurité ou rafraîchissez vos connaissances grâce à des formations audiovisuelles courtes et très captivantes.

Simulateur de phishing

Organisez des simulations d'attaques de phishing avant, pendant et après la formation afin d'évaluer la capacité des employés à résister aux cyberattaques.

Plan de cours

Des modules proposant différents types d'activités pour optimiser la mémorisation

Une solution facile à gérer pour les organisations de toutes tailles

Prise en main simple

Inscrivez-vous en ligne et bénéficiez d'un accès à la version d'essai pour un maximum de cinq utilisateurs pendant deux mois. Comprend un guide de démarrage et une assistance en ligne

Automatisation complète

Les modules de formation, les tests et les simulations de phishing sont attribués automatiquement, en fonction des paramètres du groupe de formation

Gestion proactive des risques humains

Une intégration transparente avec Kaspersky SIEM et XDR, ainsi que des API pour l'intégration avec des applications tierces, permettent d'obtenir une vue d'ensemble du comportement des employés et d'attribuer des formations en fonction de véritables incidents de sécurité, directement depuis la console

Prise en charge multilocataires et rôles d'administration flexibles

Idéal pour les organisations disposant de filiales et d'équipes réparties sur plusieurs sites, ce système permet d'assurer une supervision centralisée tout en déléguant la gestion aux administrateurs locaux.

Regroupement automatisé des utilisateurs selon des règles personnalisées prédéfinies

Organisez les formations par rôle, service ou profil de risque

Rapports clairs

Les tableaux de bord fournissent des données essentielles, avec des vues détaillées sur la progression, les retards ou les insuffisances de chaque employé, ainsi qu'un rapport PDF prêt à envoyer à la direction en un seul clic

Déploiement flexible

Disponible sous forme de plateforme SaaS ou en installation sur site

Intégration fluide

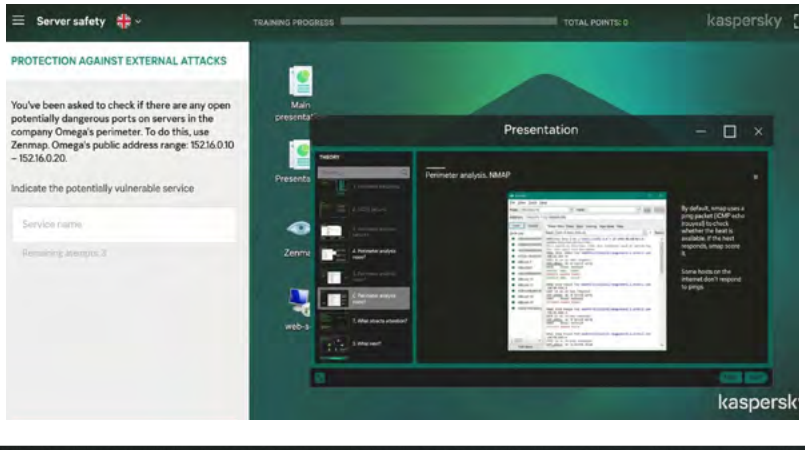
Compatible avec Active Directory et l'authentification unique (SSO)

Cybersécurité pour les services informatiques en ligne

Cybersecurity for IT Online (CITO) est un programme de formation interactif qui permet aux spécialistes des services d'assistance, aux administrateurs système et aux membres non spécialisés des équipes de sécurité informatique d'acquérir les compétences pratiques nécessaires pour détecter les cyberattaques dissimulées dans les incidents informatiques courants, collecter les données pertinentes et jouer le rôle de première ligne de défense contre les cyberattaques.

Compétences pratiques pour la gestion des incidents de premier niveau :

- Apprenez à détecter, analyser et contrer les programmes malveillants, les programmes potentiellement indésirables, les failles d'exploitation et les attaques de phishing
- Utilisez des techniques et des outils concrets pour renforcer la sécurité de l'infrastructure informatique et mener efficacement vos enquêtes sur les incidents
- Développez vos compétences en matière d'analyse des journaux, de collecte de preuves numériques et d'enquête sur les menaces
- Apprenez à sécuriser les serveurs et Active Directory grâce au renforcement de la sécurité, à la configuration des stratégies et à la surveillance



Les participants suivent six modules qui allient une partie théorique concise, des conseils pratiques et 4 à 13 exercices par module, axés sur des outils de sécurité informatique réels et des tâches quotidiennes.

Logiciels malveillants	Programmes et exploits potentiellement indésirables	Sécurité du serveur
Notions de base sur les enquêtes	Phishing et renseignements de sources ouvertes	Sécurité d'Active Directory

Kaspersky Executive Training

Encouragez une culture de la sécurité descendante en montrant comment les décisions de la direction influencent directement l'exposition aux risques, la conformité réglementaire et la résilience à long terme de l'organisation.

La formation Kaspersky Executive Training est un atelier en présentiel destiné aux dirigeants d'entreprise et aux cadres supérieurs, qui explique les implications du paysage actuel des menaces pour votre entreprise, les mesures à prendre en cas de cyberattaque, et bien plus encore. Au-delà des principes fondamentaux de la cybersécurité, les participants acquièrent une vision claire de la pertinence financière des investissements en matière de sécurité, ce qui permet aux dirigeants de faire le lien entre la protection et les performances de l'entreprise. L'idéal est de combiner cette formation avec KIPS.

Les aspects essentiels de la cybersécurité en entreprise expliqués dans un langage clair, accessible et non technique :

- Cernez la cybersécurité dans le cadre d'un système global
- Découvrez comment les cyberrisques influencent les activités de l'entreprise et comment les gérer
- Comprenez le rôle de la direction générale dans la gouvernance de la cybersécurité

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

Le programme KIPS sensibilise aux risques et aux défis liés à l'utilisation de tous types de systèmes informatiques et de processus opérationnels. Il s'agit d'un jeu interactif en équipe d'une durée de deux heures destiné aux cadres supérieurs, aux experts en systèmes d'entreprise et aux professionnels de l'informatique. Les scénarios propres à chaque secteur plongent les participants dans des techniques d'attaque modernes observées par des experts de Kaspersky lors de campagnes actives, notamment les attaques contre la chaîne d'approvisionnement, l'exploitation d'accès tiers, l'ingénierie sociale ou les programmes malveillants. Confrontées à des contraintes de temps et de budget, les équipes doivent élaborer des stratégies, anticiper les conséquences des incidents de sécurité et réagir efficacement afin de préserver les performances et le chiffre d'affaires de l'entreprise.

- Favorise la compréhension entre les décideurs
- Aide à visualiser les risques de cybersécurité et à les relier directement aux revenus et aux opérations
- Sensibilise les équipes aux questions de cybersécurité et favorise une culture axée sur la sécurité

14 scénarios propres à différents secteurs, avec de nouveaux scénarios ajoutés régulièrement

- Aéroport
- Entreprise
- Banque
- Pétrole et gaz
- Transports
- Centrale électrique
- Usine de traitement de l'eau
- Administration publique locale
- Industrie pétrochimique
- Réservoirs de pétrole
- Petites et moyennes entreprises
- Télécommunications
- Attribution technique
- Informatique

KIPS Live

Une activité divertissante qui peut être organisée en tant qu'événement autonome ou dans le cadre d'une conférence, d'un séminaire ou d'un événement d'entreprise déjà prévu.

- Jusqu'à 100 participants, par équipes de 4 à 5 personnes
- Intervenant sur site et assistant à la formation

KIPS Online

Une version en ligne est idéale pour les organisations internationales ou les activités publiques. Elle peut également être associée à KIPS Live pour permettre à des équipes à distance de participer à un événement sur site.

- Jusqu'à 300 équipes (1000 participants) de n'importe quel lieu

Options de personnalisation KIPS

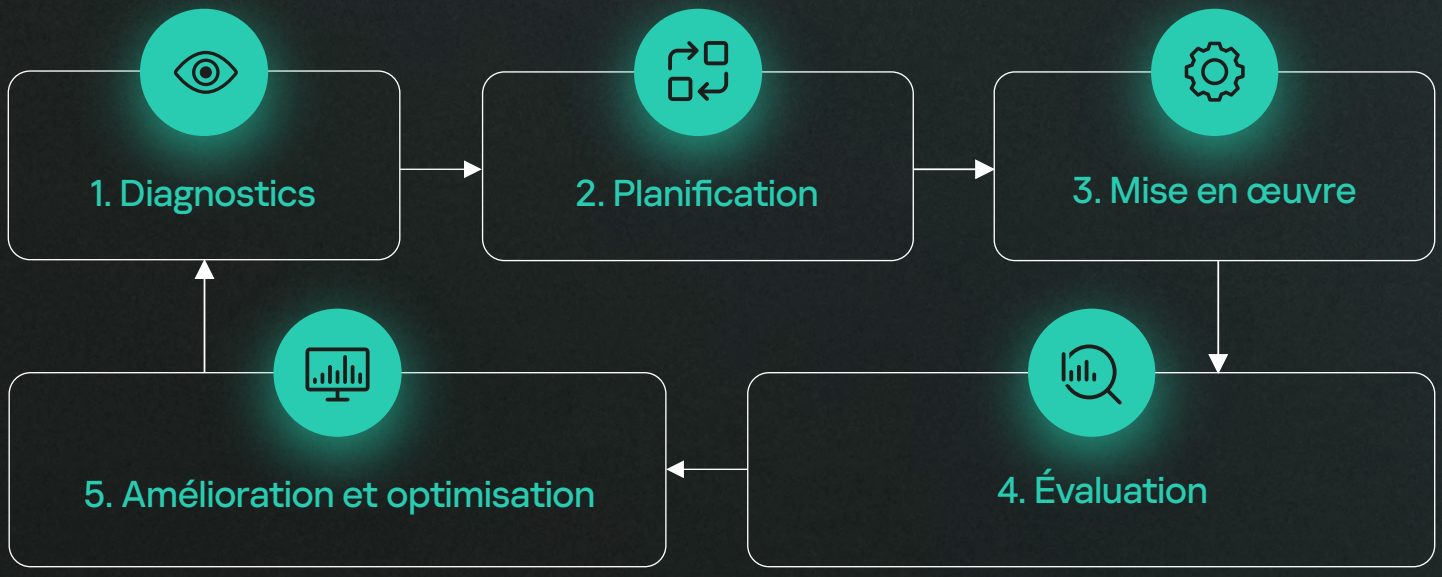
- Plateaux, cartes et numéros de table co-brandés ou aux couleurs du client
- Un scénario unique, développé en partenariat avec Kaspersky, capable de reproduire votre réseau, des incidents passés ou des menaces propres à votre secteur

Concevoir une culture de cybersécurité

La véritable cyberrésilience ne se résume pas à des stratégies et à des technologies : c'est avant tout une question de culture. Et cette culture est façonnée par l'attitude des gens, l'approche des dirigeants, la conception des processus et la manière dont la technologie vient soutenir l'ensemble :

- Les personnes et leur attitude
- Leadership et coopération
- Intégration opérationnelle
- Mise en place et préparation de la sécurité

Une culture durable de la cybersécurité repose sur un engagement constant. C'est pourquoi nous avons mis au point une approche systématique en cinq étapes essentielles, dans le cadre de laquelle vous pouvez utiliser les solutions Kaspersky Security Awareness.



Quel est le niveau actuel de maturité de la cyberculture au sein de votre organisation ?

0 Fragmenté
Risque : l'absence de pratiques et de structures de base engendre un niveau élevé de vulnérabilité. Même un incident mineur peut avoir de graves conséquences.

1 Conscient et réactif
Risque : seules les règles explicitement prescrites sont respectées. Dans les situations inhabituelles, les employés agissent selon leur propre jugement.

2 Managed
Risque : le nombre d'incidents est en baisse, mais le système reste vulnérable face à des scénarios plus complexes.

3 Intégré
Risque : les processus semblent fonctionner correctement, mais si la cyberculture ne peut pas s'autoréguler, un « risque de décalage » subsiste.

4 Puissant
Résultat : le nombre et la gravité des incidents continuent de diminuer. L'organisation est capable de s'adapter rapidement à l'évolution du paysage des menaces.

Développez dès maintenant une culture de cyberrésilience en alignant vos équipes, vos processus et vos technologies avec Kaspersky ASAP.

Essayer dès maintenant

Lorsque la sécurité cesse d'être une simple campagne pour devenir une véritable culture d'entreprise, les risques diminuent, et les résultats suivent.

RSSI

Services d'engagement client

Kaspersky Security Awareness

Soyez vigilant.
Soyez prudents.

www.kaspersky.fr

#kaspersky
#cybersecuritytruetobusiness