Formation efficace pour les employés. Facilité d'utilisation pour les administrateurs.

k-asap.fr

Kaspersky ASAP : Automated Security Awareness Platform

kaspersky BRING ON THE FUTURE

Kaspersky Automated Security Awareness Platform

Kaspersky ASAP : Automated Security Awareness Platform

Plus de 80 % de l'ensemble des cyberincidents sont dus à des erreurs humaines, et les entreprises perdent des millions pour se remettre d'incidents liés au personnel. L'efficacité des programmes de formation traditionnels destinés à prévenir ces problèmes est limitée, et bien souvent, ces derniers ne parviennent pas à favoriser le comportement nécessaire.

L'erreur humaine est le plus grand risque informatique

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

132 000 $
par PME
Impact financier moyen des violations de données causées par la perte physique d'appareils mobiles appartenant à l'entreprise et exposant l'organisation à des risques*

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*

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

26 %
des salariés
ont déclaré que leur adresse email personnelle utilisait le même mot de passe que leur compte professionnel**

Obstacles au lancement d'un programme de sensibilisation à la sécurité efficace

Si les entreprises sont disposées à mettre en œuvre des programmes de sensibilisation aux questions de sécurité, beaucoup sont mécontentes du processus et des résultats. Les petites et moyennes entreprises, qui n'ont habituellement pas l'expérience et les ressources nécessaires, sont les plus à plaindre dans ce domaine.

Pas efficaces pour les apprenants

Perçus comme difficiles, ennuyeux et assimilables à une corvée superflue.

Uniquement des interdictions plutôt que des explications

Les connaissances ne sont pas retenues

La lecture et l'écoute ne sont pas aussi efficaces que l'action

Un fardeau administratif

Comment créer un programme et fixer des objectifs

Comment gérer les missions de formation

Comment contrôler les progrès

Comment donner réellement envie aux gens de suivre des formations

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

** https://www.beyondidentity.com/blog/password-sharing-work

Efficacité et facilité de gestion de la formation pour les entreprises de toutes tailles

Présentation de la solution Automated Security Awareness Platform, qui constitue l'épine dorsale du programme de formation Kaspersky Security Awareness.

Cette plateforme est un outil en ligne aidant les salariés à développer des compétences pratiques et solides en matière de cyberhygiène tout au long de l'année. Le lancement et la gestion de la plateforme ne requièrent aucune ressource ni disposition spécifique. Cette plateforme fournit à l'entreprise une aide intégrée à chaque étape de son parcours vers un cyberenvironnement d'entreprise sûr.

Comment évaluer un programme de sensibilisation

L'un des critères déterminants dans le choix d'un programme de sensibilisation est son efficacité. Avec ASAP, l'efficacité est intrinsèque au contenu et à la gestion de la formation. Le contenu de la plateforme est composé de plus de 300 compétences pratiques et indispensables en matière de cybersécurité, que tous les salariés doivent acquérir.

Sensibilisez vos employés aux problèmes de cybersécurité afin de changer leur attitude et leur comportement, et protégez votre entreprise et vos systèmes informatiques.

Formation efficace

Cohérente	– Contenu bien pensé et structuré – Des cours interactifs, un renforcement constant, des tests et des simulations d'attaques par phishing pour veiller à l'application des compétences Les documents de formation et leur structure sont présentés conformément aux particularités de la mémoire humaine, autrement dit, à notre capacité à assimiler et à retenir l'information.
Pratique et motivante	– Pertinente pour le travail quotidien des salariés – Des compétences qui peuvent être mises en pratique immédiatement Des exemples de situations réelles dans lesquelles les salariés peuvent se reconnaître contribuent à l'engagement des utilisateurs tout en les aidant à retenir l'information.
Positive	– Permet d'inculquer de manière proactive des comportements plus sûrs – Explique « pourquoi » et « comment » au lieu d'interdire Trop de règles et de restrictions peuvent susciter le mécontentement, tandis que des explications et des convictions en adéquation avec le mode de pensée naturel des utilisateurs contribuent à leur adhésion et à la modification de leur comportement.

Administration simplifiée

Gestion simplifiée	La gestion entièrement automatisée des formations aide tous les salariés à atteindre les compétences en matière de sécurité adaptées à leur profil, sans aucune intervention de l'administrateur de la plateforme
Contrôle simplifié	Tableau de bord « tout-en-un » et rapports exploitables
Participation simplifiée	Des invitations et des emails de motivation, ainsi que des rapports hebdomadaires destinés aux administrateurs et aux utilisateurs, sont envoyés automatiquement par la plateforme.

Gestion ASAP : simplicité grâce à une automatisation complète

Démarrez votre programme en 4 étapes simples

Télécharger les utilisateurs

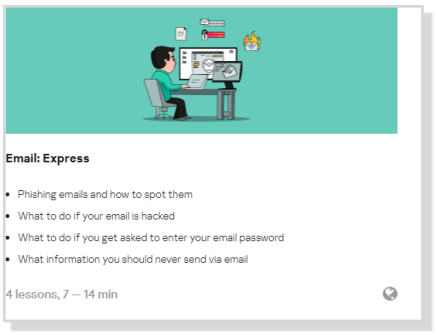
Répartir les utilisateurs par profil de risque et définir des niveaux cibles pour chaque groupe

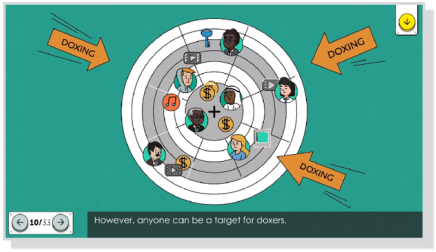
La seule étape exigeant une réflexion et une prise de décision de la part de l'administrateur

Lancer la formation

Gestion des formations automatisé effectuée par ASAP

La plateforme crée un programme de formation pour chaque groupe, en fonction du rythme et du niveau cible, et fournit des recommandations et des rapports exploitables





De meilleurs principes d'apprentissages

Kaspersky ASAP change la façon dont nous fournissons du contenu de formation à la cybersécurité. Vous pouvez désormais choisir d'attribuer aux salariés une formation express de base qui vous permettra de répondre rapidement aux exigences réglementaires en matière de formation à la cybersécurité, ou de rafraîchir leurs connaissances, ou d'opter pour une formation complète déclinée en plusieurs niveaux de complexité

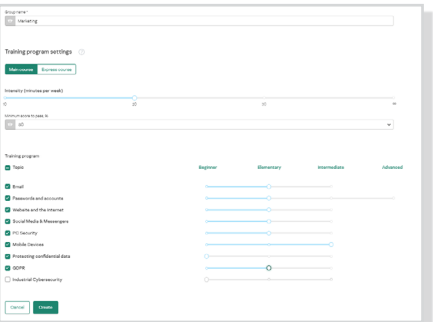
Formation express

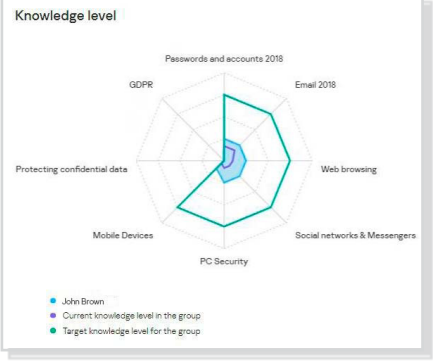
Une version courte de la formation au format audio-vidéo. Chacun des 6 grands thèmes de la cybersécurité contient plusieurs petits cours pour aider l'utilisateur à maîtriser les compétences de base en matière de cybersécurité.
– Théorie interactive
– Vidéos
– Tests
Les attaques de phishing simulées ne sont pas incluses dans le parcours d'apprentissage, mais peuvent être attribuées en plus par l'administrateur

Parcours d'apprentissage spécifiques pour chaque profil de risque

Utilisez des règles automatisées pour affecter des salariés à un certain groupe en fonction du niveau de formation cible souhaité. Ce niveau cible dépend du risque pour l'entreprise que représente une fonction. Plus le risque est élevé, plus le niveau de formation cible doit être élevé. Par exemple, les informaticiens et les comptables représentent généralement un risque plus élevé que les autres salariés.

Une gestion flexible des formations





Formation souple

- Le domaine de formation est entièrement flexible, tout en conservant les avantages de la gestion automatisée et séquentielle des formations
- Pour chaque groupe de formation, vous pouvez sélectionner :
  - La formation principale ou express, ou une combinaison des deux
  - Les thèmes à aborder dans la formation principale et/ou la formation express que les participants du groupe doivent apprendre
  - Le niveau cible que vous souhaitez que les apprenants atteignent pour chaque thème sélectionné dans la formation principale.

Rapports exploitables à tout moment

- Profitez de tableaux de bord contenant toutes les informations requises pour contrôler et gérer les synthèses statistiques relatives aux utilisateurs de l'entreprise, les emplacements de formation et les formations de groupe, avec la possibilité de passer à un niveau individuel
- Recevez des suggestions d'amélioration des résultats
- Téléchargez d'un simple clic les rapports sur la page principale, et configurez la fréquence de réception des rapports par email

La liberté d'exceller

Les salariés peuvent suivre leur formation à tout moment et à partir de n'importe quel appareil. Grâce à une conception adaptée aux mobiles, l'apprentissage est encore plus confortable. Les utilisateurs peuvent accéder au portail de formation en utilisant des liens personnalisés à partir de l'invitation à la formation ou en utilisant un lien unique pour tous les utilisateurs à l'aide de la technologie d'authentification unique (SSO)

Méthodologie de la formation principale ASAP

Apprentissage incrémentiel en continu

- Du plus simple au plus complexe, thème par thème et niveau par niveau : les connaissances augmentent
- Élargissement et application des connaissances déjà acquises dans de nouveaux contextes

Contenu multimodal

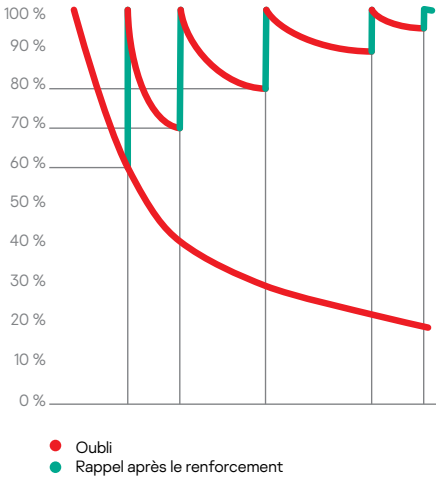
- Chaque niveau inclut : évaluation de l'apprentissage via des cours interactifs (test et simulation d'attaque par phishing, le cas échéant)
- Tous les éléments de formation étayent la compétence particulière développée dans chaque unité, de sorte que les compétences soient totalement maîtrisées et fassent partie intégrante du nouveau comportement souhaité

Apprentissage par intervalles

- La courbe de l'oubli d'Ebbinghaus : méthode d'apprentissage fondée sur les particularités de la mémoire humaine
- La répétition crée des comportements sûrs et aide à retenir l'information
- Renforcement dans chaque module

La courbe de l'oubli d'Ebbinghaus

Le renforcement répété contribue à développer de solides compétences.



Chaque thème comprend plusieurs niveaux, chacun comportant une description des compétences en matière de sécurité. Les niveaux sont définis en fonction du degré de risque qu'ils contribuent à éliminer : le niveau 1 est normalement suffisant pour se protéger des attaques les plus simples et des attaques de masse. Pour se protéger des attaques les plus complexes et les plus ciblées, il convient de suivre les niveaux supérieurs.

Thèmes de formation

- 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

Exemple : Compétences enseignées dans le thème « Sites Web et Internet »

Débutant Éviter les attaques massives (bon marché et faciles)	**Élémentaire** Éviter les attaques massives sur un profil spécifique	**Intermédiaire** Éviter les attaques ciblées bien préparées	**Avancé*** Éviter les attaques ciblées
23 compétences, notamment : – Reconnaître les fausses fenêtres contextuelles – Faire attention aux redirections – Distinguer les liens de téléchargement authentiques des faux – Reconnaître les fichiers exécutables trouvés sur le Web – Être capable de déterminer l'authenticité d'une extension de navigateur	**34 compétences, notamment :** – Saisir des données uniquement sur les sites disposant d'un certificat SSL valide – Utiliser des mots de passe variés pour les différentes inscriptions – Reconnaître les faux sites par un certain nombre de signes - Éviter les liens numériques – Reconnaître les adresses de liens réseau invalides par la présence de faux sous-domaines	**12 compétences, notamment :** – Vérifier les liens de partage avant de les envoyer – Utiliser uniquement des logiciels de fabricants fiables pour télécharger des torrents – Télécharger uniquement du contenu légal à partir des torrents – Effacer régulièrement les cookies des navigateurs	**13 compétences, notamment :** - Reconnaître des liens contrefaits sophistiqués (dont des liens ressemblant au site Web de votre entreprise et des liens avec redirections) – Vérifier les sites à l'aide d'utilitaires spéciaux – Reconnaître si le navigateur est en train de faire du minage – Éviter des sites référencés sur liste noire
	+ renforcement des compétences élémentaires	+ renforcement des compétences précédentes	+ renforcement des compétences précédentes

Principaux points abordés dans le thème : liens, téléchargements, installations de logiciels, inscription et identification, paiements et SSL

* Ajout prévu dans le courant de l'année 2022

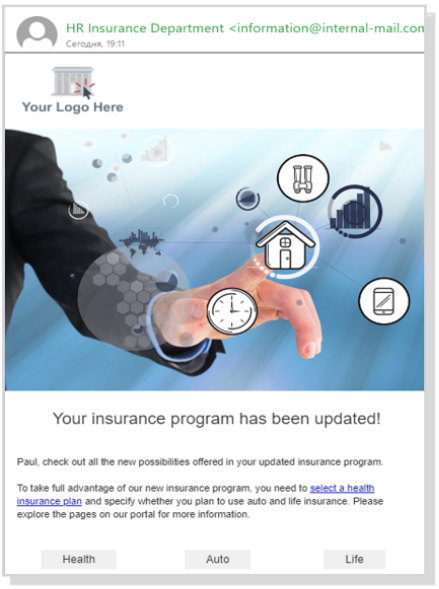
Langues disponibles

La plateforme (interface administrateur et utilisateur) est disponible dans les langues suivantes :

- Arabe
- Néerlandais
- Anglais
- Français
- Allemand
- Italien
- Portugais
- Russe
- Espagnol
- Tchèque
- Kazakh
- Polonais
- Slovène
- Roumain
- Turc
- Hongrois
- Danois
- Suédois
- Grec*
- Serbe
- Portugais (Brésil)*
- Portugais
- Roumain
- Serbe
- Slovène
- Suédois
- Turc
- Grec
- Japonais
- Chinois (mandarin)*

* Prévu pour 2022

Exemple de modèle de phishing simulé modifiable et de commentaires



Un contenu équilibré, structuré et pertinent par rapport aux situations réelles est synonyme d'efficacité

Les principes d'apprentissage d'ASAP se fondent sur la méthodologie qui prend en compte les spécificités de la nature humaine, dont notre capacité à percevoir et à assimiler l'information. Le contenu regorge d'exemples et de cas réels qui mettent en évidence l'importance personnelle de la cybersécurité pour les employés.
La plateforme met l'accent sur le développement des compétences et non uniquement sur la mise à disposition de connaissances. Les exercices pratiques sont donc au cœur de chaque module.

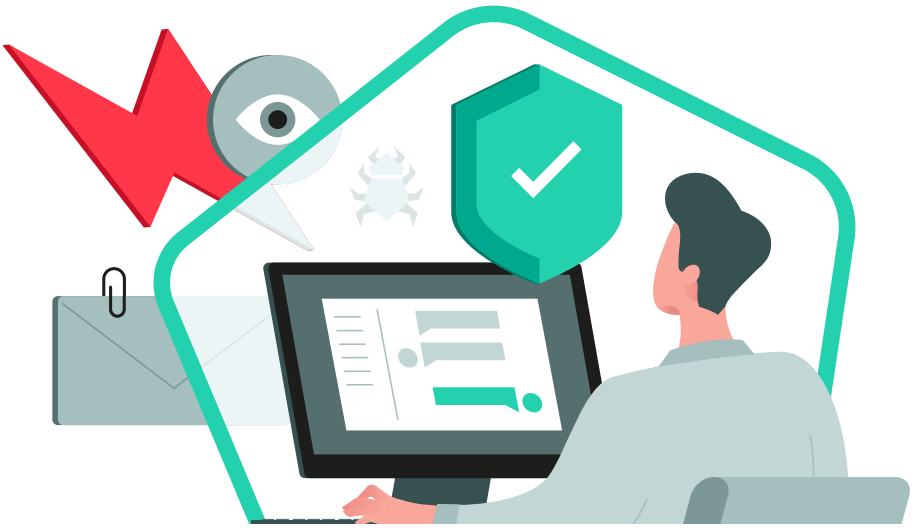
Le style visuel et les textes sont non seulement traduits dans différentes langues, mais sont aussi ajustés pour tenir compte des différentes cultures et mentalités locales.

Simulations de campagnes de phishing

Les campagnes de phishing sont un complément au processus de formation principal qui permet de tester les compétences pratiques des employés pour éviter les attaques par phishing. Le responsable de la formation pourra ainsi déterminer les lacunes dans les connaissances des utilisateurs et les encourager à étudier les thèmes qui leur posent problème.

La plateforme propose des modèles d'emails prêts à l'emploi contenant des exemples de phishing qui peuvent être envoyés aux utilisateurs de la plateforme dans toutes les langues disponibles. Les modèles disponibles sont régulièrement mis à jour et renouvelés. Vous pouvez également créer des emails personnalisés à partir de modèles prédéfinis.

Essayez de simuler une attaque de phishing avant de commencer la formation – vérifiez la résilience de vos employés ! Cette action permettra aux salariés et à la direction de constater les avantages de la formation.



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

Principaux facteurs de différenciation des programmes

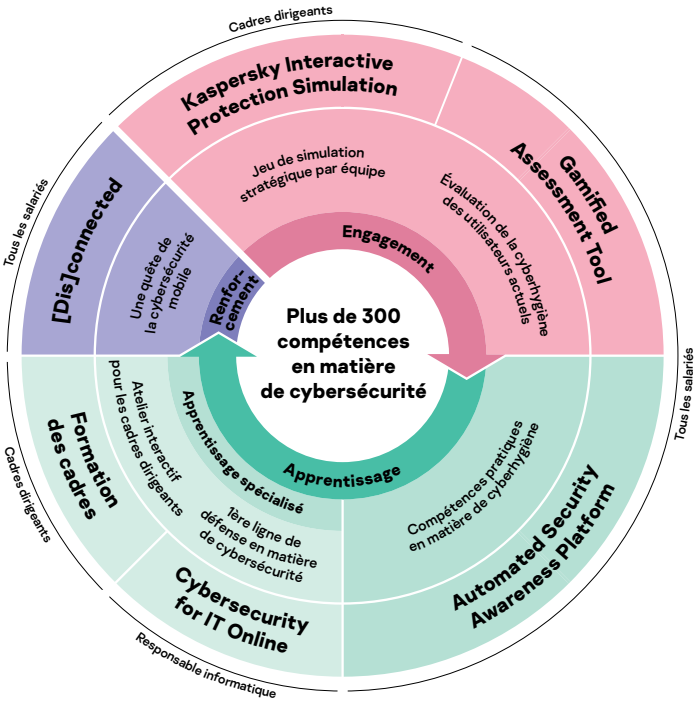
Une expertise considérable en matière de cybersécurité
Plus de 20 ans d'expérience dans le domaine de la cybersécurité transformés en un ensemble de compétences de cybersécurité qui est au cœur de nos produits

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.

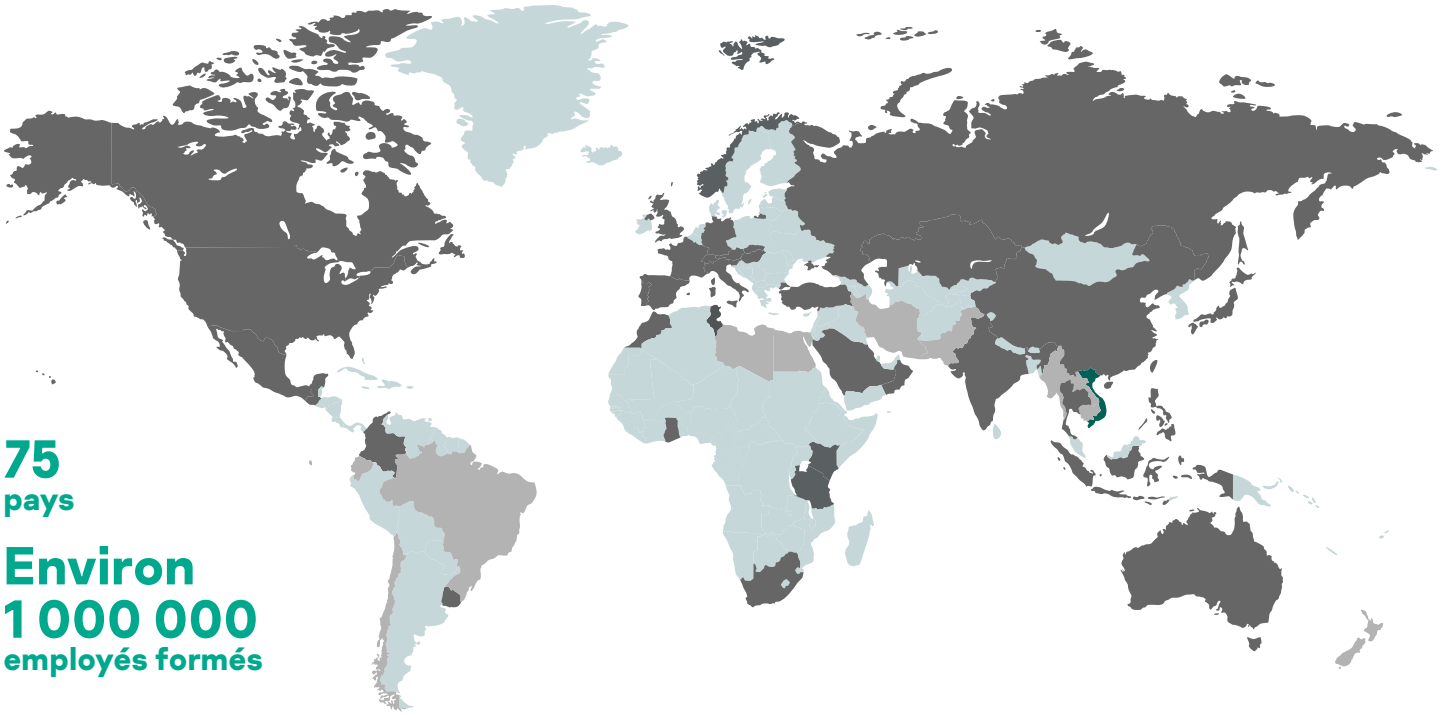
Kaspersky Security Awareness propose un éventail de solutions qui couvrent l'ensemble des besoins spécifiques des entreprises en matière de cybersécurité et enseigne les compétences que chaque membre du personnel devrait maîtriser en s'appuyant sur les dernières techniques et technologies d'apprentissage.

Une solution de formation flexible accessible à tous

Choisissez une solution unique qui répond à un besoin de sécurité spécifique, ou laissez-nous vous fournir une offre simplifiant le lancement et le ciblage de vos formations sur la base de vos besoins et de vos priorités. Vous trouverez de plus amples informations sur les forfaits à l'adresse suivante : https://www.kaspersky.fr/enterprise-security/security-awareness



Kaspersky Security Awareness dans le monde



75
pays

Environ
1 000 000
employés formés

Kaspersky ASAP essai gratuit : k-asap.fr
Solutions de cybersécurité pour les entreprises : www.kaspersky.fr/enterprise-security
Kaspersky Security Awareness : www.kaspersky.fr/enterprise-security/security-awareness
Actualités dédiées à la sécurité informatique : www.kaspersky.fr/blog/category/business/

www.kaspersky.fr

kaspersky BRING ON THE FUTURE