

Efficacité
et facilité de
gestion pour les
entreprises
de toutes tailles

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.

Les erreurs humaines sont considérées aujourd'hui comme le plus grand risque de cybersécurité

1 057 000 \$

par entreprise/organisation

Impact financier moyen des violations de données causées par une mauvaise utilisation des ressources informatiques par les salariés*

98 000 \$

par PME

Impact financier moyen des violations de données causées par une mauvaise utilisation des ressources informatiques par les salariés*

52 %

des entreprises

considèrent les salariés comme la principale menace pour la cybersécurité en entreprise**

30 %

des salariés

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***

Les 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 élèves :



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 : « 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, 2019

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

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

Gestion de la sensibilisation efficace et simplifiée 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 environnement de cybersécurité 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 basé sur un modèle de compétences composé de 350 compétences pratiques et indispensables en matière de cybersécurité, que tous les salariés doivent acquérir. S'ils ne développent pas ces compétences, que ce soit par ignorance ou par négligence, les salariés représentent un danger pour l'entreprise.

Formation efficace

Cohérente

- Contenu bien pensé et structuré
- Des leçons interactives, 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 de risque, sans aucune intervention de l'administrateur de la plateforme.

Contrôle simplifié

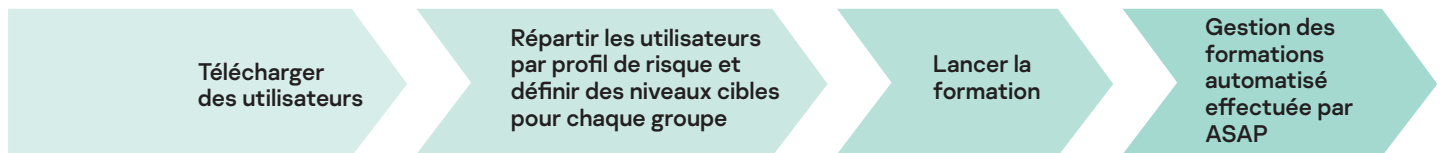
Tableau de bord « tout-en-un » et rapports exploitables

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 : la simplicité par une automatisation complète

Démarrez votre programme en 4 étapes simples

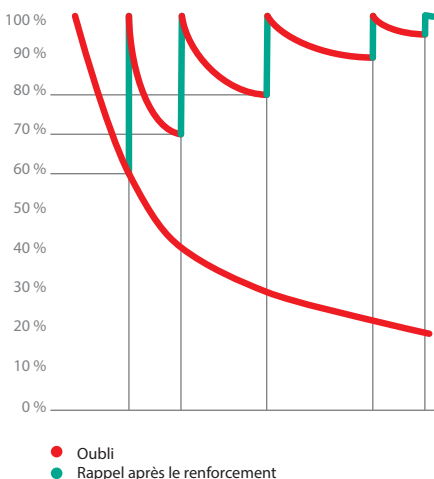


La seule étape exigeant une réflexion et une prise de décision de la part de l'administrateur

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

La courbe de l'oubli d'Ebbinghaus

Le renforcement répété contribue à développer de solides compétences.



S'adapte au rythme individuel et aux capacités d'apprentissage de chaque salarié

- La plateforme s'assure automatiquement que les utilisateurs apprennent les bases et réussissent les tests correspondants avant de passer au prochain niveau
- L'équipe de direction n'a pas besoin de passer du temps sur l'analyse des progrès individuels et les réglages manuels

Bénéficier de 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.

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 :
 - les thèmes que les membres du groupe doivent connaître (en ignorant ceux que vous ne souhaitez pas qu'ils maîtrisent pour l'instant) ;
 - le niveau cible que vous souhaitez que les utilisateurs atteignent pour chaque thème en particulier.Les salariés ne doivent pas passer leur temps de travail sur des thèmes de formation inutiles.

Obtenir des rapports exploitables à tout moment

- Bénéficier de tableaux de bord contenant toutes les informations nécessaires au contrôle
- Recevoir des suggestions d'amélioration des résultats
- Télécharger d'un simple clic les rapports sur la page principale, et configurer la fréquence de réception des rapports par courrier

Méthodologie 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 comprend : Évaluation de renforcement des leçons interactives (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
- La courbe de l'oubli d'Ebbinghaus : méthodes d'apprentissage fondées sur les particularités de la mémoire humaine
- La répétition crée des comportements sûrs et aide à retenir l'information
- Renforcement dans chaque module

Apprentissage par intervalles

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

Thèmes de formation

Chaque thème comprend plusieurs niveaux, chacun comportant une description des compétences en matière de sécurité. Les niveaux sont définis selon les degrés de risque qu'ils visent à éliminer : le niveau 1 est généralement suffisant pour éviter les attaques les plus courantes et massives, alors que pour une protection contre les attaques plus sophistiquées et ciblées, il convient d'étudier les niveaux suivants.

- Mots de passe et comptes
- Email
- Navigation sur Internet
- Réseaux sociaux et messageries instantanées
- Sécurité pour PC
- Appareils mobiles
- Données confidentielles*
- RGPD*

* Ajout prévu dans IQ 2020

Exemple : compétences développées dans le thème « Navigation sur 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
<p>13 compétences, notamment :</p> <ul style="list-style-type: none"> - Configurer votre PC (mises à jour, antivirus) - Ignorer les sites Web malveillants évidents (ceux qui demandent de mettre à jour le logiciel, d'optimiser les performances du PC, d'envoyer des SMS, d'installer des lecteurs, etc.) - Ne jamais ouvrir les exécutables depuis des sites Web 	<p>20 compétences, notamment :</p> <ul style="list-style-type: none"> - S'inscrire/Se connecter uniquement sur les sites de confiance - Éviter les liens numériques - Saisir des informations sensibles sur des sites de confiance uniquement - Reconnaître les signes d'un site Web malveillant 	<p>14 compétences, notamment :</p> <ul style="list-style-type: none"> - Reconnaître des liens contrefaits - Reconnaître des fichiers et téléchargements malveillants - Reconnaître des logiciels malveillants 	<p>13 compétences, notamment :</p> <ul style="list-style-type: none"> - Reconnaître des liens contrefaits sophistiqués (dont des liens ressemblant au site Web de votre entreprise et des liens avec redirections) - Éviter des sites référencés sur liste noire - Se déconnecter lorsque vous avez terminé - Configuration avancée du PC (désactiver Java, adblock, noscript, etc.)
	+ renforcement des compétences élémentaires	+ renforcement des compétences précédentes	+ renforcement des compétences précédentes

Principaux sujets couverts dans ce thème : Liens, Téléchargements, Installations de logiciels, Inscription et connexion, Paiements, SSL

Langues disponibles

À compter de juillet 2019, la plateforme (interface administrateur et utilisateur) est disponible dans les langues suivantes :

- Arabe
- Néerlandais
- Anglais
- Français
- Allemand
- Italien
- Portugais
- Russe
- Espagnol

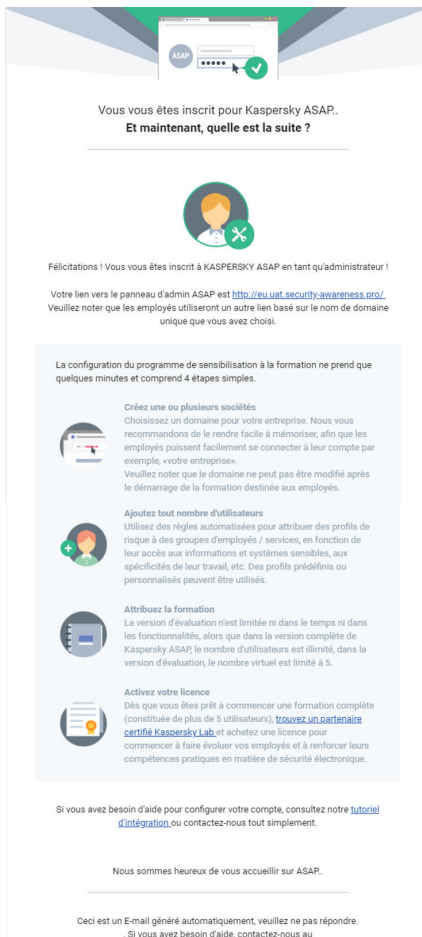
Un contenu équilibré, structuré et pertinent par rapport aux situations réelles est synonyme d'efficacité

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 fourmille d'exemples pratiques qui mettent en évidence l'importance de la cybersécurité pour les salariés. La plateforme met l'accent sur le développement de compétences, et non seulement sur la diffusion de connaissances. Les exercices pratiques et les tâches spécifiques des salariés sont donc au cœur de chaque module.

Les modules combinent différents types d'exercices aidant les utilisateurs à rester intéressés et alertes, tout en les incitant à apprendre et à acquérir des comportements sûrs.

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.

Tâches et exercices basés sur la simulation afin de développer des compétences pratiques et de continuer à divertir et à motiver les utilisateurs



Vous vous êtes inscrit pour Kaspersky ASAP.
Et maintenant, quelle est la suite ?

Félicitations ! Vous vous êtes inscrit à KASPERSKY ASAP en tant qu'administrateur !
Votre lien vers le panneau d'admin ASAP est <http://eu.uat.securityawareness.pro/>.
Veuillez noter que les employés utiliseront un autre lien basé sur le nom de domaine unique que vous avez choisi.

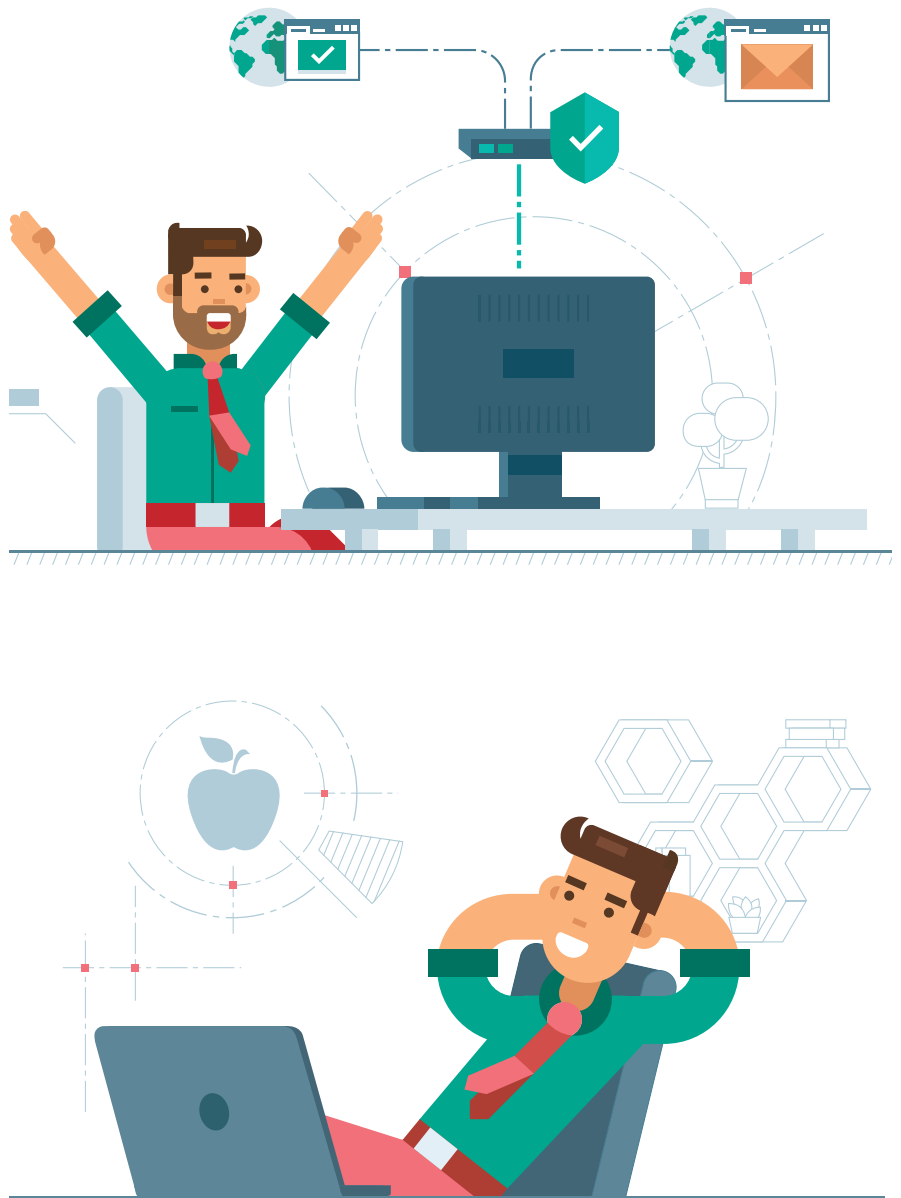
La configuration du programme de sensibilisation à la formation ne prend que quelques minutes et comprend 4 étapes simples.

- Créez une ou plusieurs sociétés**
Choisissez un domaine pour votre entreprise. Nous vous recommandons de le rendre facile à mémoriser, afin que les employés puissent facilement se connecter à leur compte par exemple, «votre entreprise».
Veuillez noter que le domaine ne peut pas être modifié après le démarrage de la formation destinée aux employés.
- Ajoutez tout nombre d'utilisateurs**
Utilisez des règles automatisées pour attribuer des profils de risque à des groupes d'employés / services, en fonction de leur accès aux informations et systèmes sensibles, aux spécificités de leur travail, etc. Des profils prédéfinis ou personnalisés peuvent être utilisés.
- Attribuez la formation**
La version d'évaluation n'est limitée ni dans le temps ni dans les fonctionnalités, alors que dans la version complète de Kaspersky ASAP le nombre d'utilisateurs est illimité, dans la version d'évaluation, le nombre virtuel est limité à 5.
- Activez votre licence**
Dès que vous êtes prêt à commencer une formation complète (constituée de plus de 5 utilisateurs), [trouvez un partenaire certifié Kaspersky Lab](#) et achetez une licence pour commencer à faire évoluer vos employés et à renforcer leurs compétences pratiques en matière de sécurité électronique.

Si vous avez besoin d'aide pour configurer votre compte, consultez notre [tutoriel d'intégration](#) ou contactez-nous tout simplement.

Nous sommes heureux de vous accueillir sur ASAP.

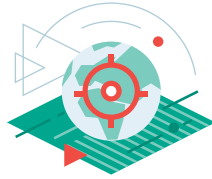
Ceci est un E-mail généré automatiquement, veuillez ne pas répondre.
...Si vous avez besoin d'aide, contactez-nous au





Kaspersky Security Awareness

Principaux facteurs de différenciation des programmes



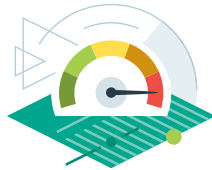
Formation ciblée, basée sur les fonctions

- Apprenez ce que vous devez savoir, selon votre fonction et votre profil de risque
- Des exemples concrets associés à des compétences qui peuvent être mises en pratique immédiatement
- Apprentissage par la pratique



Centré sur la nature humaine

- Une formation structurée selon le mode de pensée naturel des gens
- Permet d'inculquer de manière positive et proactive des comportements plus sûrs
- Des informations et des compétences faciles à assimiler et à retenir, grâce à des méthodes fondées sur les particularités de la mémoire humaine



Apprentissage incrémentiel en continu

- Du plus simple au plus complexe
- Élargissement et application des connaissances déjà acquises dans de nouveaux contextes



Facile à gérer et à contrôler

- En ligne
- Gestion des formations automatisée
- Envoi automatique d'invitations et d'emails de motivation contenant des recommandations individuelles pour chaque utilisateur

Différents formats de formation pour différents niveaux organisationnels



Kaspersky ASAP - Essai gratuit : k-asap.fr
Solutions de cybersécurité pour les entreprises : www.kaspersky.fr/entreprise
Kaspersky Security Awareness : www.kaspersky.fr/awareness
Actualités dédiées à la sécurité informatique : business.kaspersky.com

www.kaspersky.fr

kaspersky BRING ON
THE FUTURE