KASPERSKY lab

Kaspersky ASAP : Automated Security Awareness Platform

Efficacité et facilité de gestion pour les entreprises de toutes tailles

https://kas.pr/frkaspersky/asap
#truecybersecurity

Kaspersky ASAP : Automated Security Awareness Platform

Plus de 80 % des incidents informatiques sont dus à l'erreur humaine. Les entreprises perdent des millions pour se remettre d'incidents provoqués par le personnel, mais l'efficacité des programmes de formation traditionnels visant à prévenir ces problèmes est limitée et, bien souvent, ils ne réussissent pas à susciter la motivation et le comportement escomptés.

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

83 000 $ par PME

Impact financier moyen des attaques causées par des salariés négligents/mal informés [1]

101 000 $ par PME

Impact financier moyen des attaques causées par le phishing/le piratage informatique [1]

400 $ par salarié par an

Coût moyen des attaques de phishing (les autres types de cybermenaces sont exclus de ce chiffre)

52 % de toutes les entreprises

ont désigné les imprudences des salariés/utilisateurs comme le problème le plus important dans leur stratégie de sécurité informatique

[1] « Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within » (« Facteur humain dans la sécurité informatique : Comment les salariés rendent les entreprises vulnérables de l'intérieur »), Kaspersky Lab et B2B International, juin 2017

[2] Calculs établis à partir du rapport d'août 2015 du Ponemon Institute intitulé « Cost of Phishing and Value of Employee Training » (« Coût du phishing et valeur de la formation des salariés »).

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

Alors que les entreprises ont hâte de mettre en œuvre des programmes de sensibilisation aux questions de sécurité, peu d'entre elles sont satisfaites à la fois du processus et des résultats. Les petites et moyennes entreprises, qui ne disposent généralement pas de l'expérience et des ressources dédiées, sont particulièrement vulnérables.

Aucune idée de comment fixer des objectifs et planifier la formation

La gestion de la formation prend trop de temps

Les rapports ne contribuent pas au suivi des objectifs

Les salariés n'apprécient pas le programme → ne disposent pas des compétences

Même les organisations dotées d'équipes chargées de la sensibilisation éprouvent souvent des difficultés pour obtenir une réelle amélioration dans le comportement des utilisateurs, suite à une formation de sensibilisation à la sécurité.

De nombreuses sociétés choisissent entre un effort éducatif ponctuel (« tout sur la cybersécurité en 1 heure », par exemple) et des programmes de formation professionnelle bien structurés qui, toutefois, n'utilisent que quelques fonctions et instruments de base. En général, il s'agit d'un certain nombre de vagues d'attaques de phishing simulées par année, ainsi que de quelques leçons généralistes car il est trop complexe de mettre en place et de gérer des programmes plus lourds. De toute façon, les salariés ne disposent pas des compétences solides nécessaires pour créer un niveau de sécurité soutenu pour leur entreprise.

Efficacité et facilité de la gestion de la sensibilisation pour les entreprises de toute taille

Kaspersky Lab présente Automated Security Awareness Platform, qui constitue la partie essentielle du programme de formation Kaspersky Security Awareness.

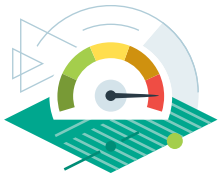
Cette plateforme est un outil en ligne qui développe des compétences pratiques et solides en matière de cyberhygiène pour les salariés tout au long d'une année. Le lancement et la gestion de la plateforme ne requièrent aucune ressource spécifique. Elle fournit à l'entreprise une aide intégrée pour toutes les étapes de son parcours vers un environnement cybernétique d'entreprise plus sûr :

Étape 1 :

Définir des objectifs de formation et justifier un programme

- Fixer des objectifs par rapport aux analyses comparatives mondiales
- Trouver un juste équilibre entre le niveau de compétence visé pour chaque groupe de salariés et le temps total d'apprentissage nécessaire pour les amener à ce niveau

Étape 2 :



Veiller à ce que tous les salariés soient formés jusqu'à atteindre leur meilleur niveau requis

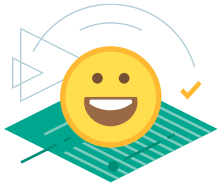
- Utiliser l'apprentissage automatisé pour permettre à chaque salarié d'atteindre le niveau de compétence correspondant à son profil de risque (faible, intermédiaire, important et critique).
- S'assurer que les compétences acquises sont renforcées pour empêcher qu'elles ne soient oubliées
- Former les salariés individuellement et à leur propre rythme de façon à éviter le surentraînement et le rejet

Étape 3 :

Surveiller les progrès effectués grâce à des rapports exploitables et à des analyses

- Obtenir un suivi en direct des données, des tendances et des prévisions
- Utiliser la prévision en temps réel pour atteindre les objectifs de formation annuels
- Répondre aux questions avant qu'elles ne deviennent des problèmes (en identifiant les secteurs de l'organisation qui méritent davantage d'attention)
- Réaliser une analyse comparative des résultats provisoires

Étape 4 :



Garantir l'appréciation de la formation et, par conséquent, son efficacité

- Faire participer les salariés à la formation grâce à des exercices pratiques (interactifs) basés sur des scénarios réels
- S'assurer que la formation est pertinente au quotidien
- Éviter la surcharge d'informations

Gestion du programme : la simplicité par l'automatisation

Démarrez le programme en 10 minutes :

- Fixez des objectifs en fonction des moyennes mondiales/du secteur
- Commencez la formation
- Ne payez que pour les utilisateurs actifs (ceux qui sont en train d'apprendre)

La plateforme s'adapte au rythme individuel et aux capacités d'apprentissage de chaque salarié

- La plateforme veille automatiquement à ce que l'utilisateur apprenne et réussisse les tests de base avant de passer à un niveau de formation plus approfondi
- L'équipe de direction n'a pas besoin de passer du temps sur l'analyse de progression individuelle et les réglages manuels

Bénéficiez de parcours d'apprentissage spécifiques pour chaque profil de risque

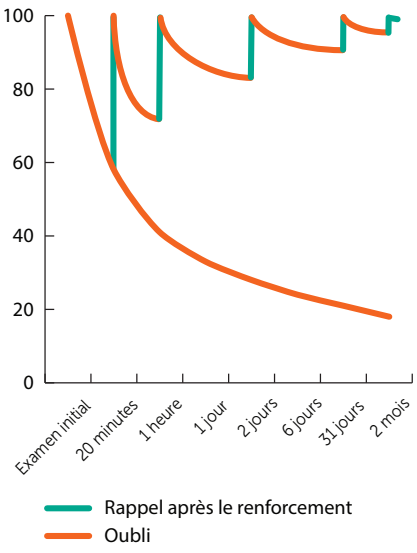
- Utilisez des règles automatisées pour affecter des profils de risque à un groupe de salariés/de services, selon leur accès aux informations et aux systèmes sensibles, leurs caractéristiques de travail, etc. Vous pouvez utiliser des profils de risque prédéfinis ou personnalisés.
- La plateforme n'assignera pas de formation excessive aux utilisateurs présentant un risque faible

Obtenez des rapports exploitables à tout moment

- Profitez de tableaux de bord contenant toutes les informations nécessaires pour évaluer les progrès
- Recevez des suggestions sur ce qu'il faut faire pour améliorer les résultats
- Comparez les résultats avec les références mondiales/de l'industrie disponibles

La courbe de l'oubli d'Ebbinghaus

Le renforcement répété contribue à développer de solides compétences.



Pour une formation efficace : micro-apprentissage continu

Les compétences se développent niveau par niveau, du plus simple au plus avancé. La plateforme réaffecte automatiquement plus de formation à ceux qui n'ont pas réussi à terminer un niveau précédent. Cela permet de consolider les compétences et d'empêcher l'oubli.

Micro-apprentissage

- Le contenu est spécialement structuré pour un micro-apprentissage (2 à 10 minutes), évitant ainsi les longues leçons ennuyeuses et laborieuses.

Ensemble complet d'outils pour chaque domaine de la sécurité

- Chaque niveau comprend : un module interactif et une évalation de renforcement en vidéo (test ou simulation d'attaque de phishing)

Chaque thème comprend 3 niveaux*, chacun comportant une description des compétences en matière de sécurité. Les niveaux sont définis selon les degrés des risques qu'ils visent à éliminer : le niveau 1 est généralement suffisant pour protéger contre les attaques les plus courantes et massives, alors que pour une protection contre les attaques plus sophistiquées et ciblées, il faut atteindre le niveau 3.

Thèmes de formation**

Email/phishing	Données confidentielles
Navigation sur Internet	Données personnelles RGPD
Mots de passe	Ingénierie sociale
Réseaux sociaux et messageries instantanées	Sécurité chez soi et en déplacement
Protection PC	
Appareils mobiles	

*un 4ème niveau sera développé prochainement
**cette liste peut être amenée à évoluer

Exemple : compétences développées dans le thème « Navigation sur Internet »

Niveau élémentaire pour éviter les attaques massives (bon marché et facile)	Niveau débutant pour éviter des attaques massives sur un profil spécifique	Niveau intermédiaire pour éviter des attaques ciblées bien préparées	Niveau avancé pour éviter les attaques ciblées
13 compétences, notamment : - 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	20 compétences, notamment : - S'inscrire/Se connecter uniquement aux sites de confiance - Éviter de cliquer sur des liens numériques - Saisir des informations sensibles sur des sites de confiance uniquement - Reconnaître les signes d'un site Web malveillant	14 compétences, notamment : - Reconnaître des liens contrefaits - Reconnaître des fichiers et téléchargements malveillants - Reconnaître des logiciels malveillants	13 compétences, notamment : - Reconnaître des liens contrefaits sophistiqués (dont des liens ressemblant au site Web de votre entreprise, des liens avec redirection) - 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

Langues disponibles :
- Français
- Anglais
- Allemand
- Italien
- Russe
- Espagnol

Prochainement
- Arabe

De nouvelles langues sont régulièrement ajoutées afin de garantir un enseignement approfondi et efficace pour tous les pays.

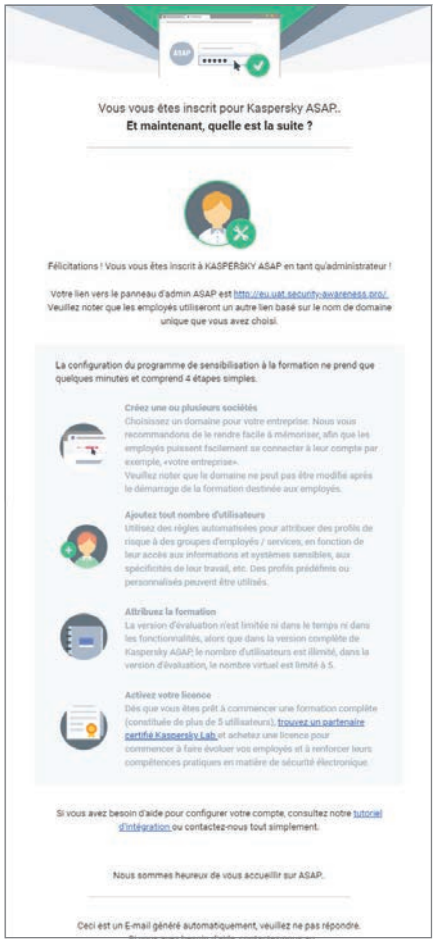
Apprentissage ludique et pertinence par rapport à la vie réelle, pour en garantir l'efficacité

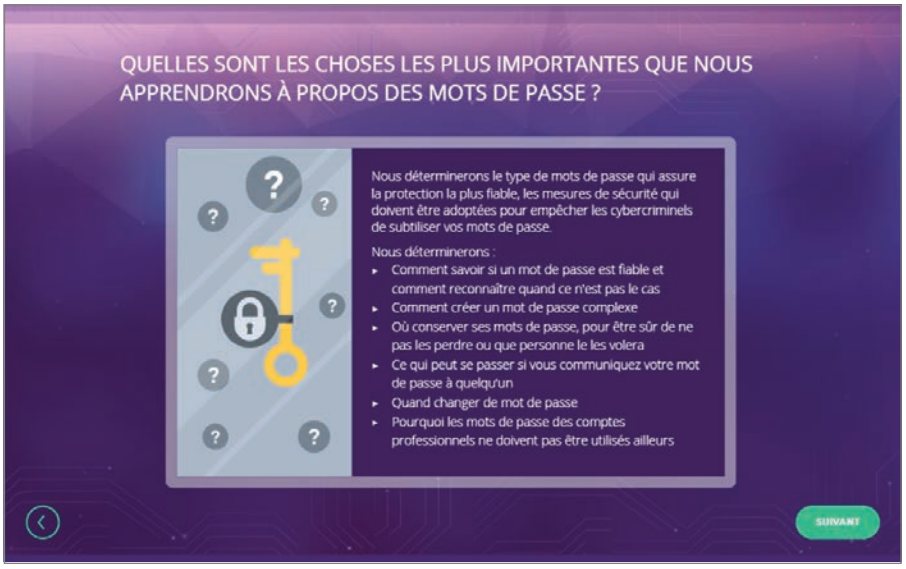
Le contenu de la plateforme se base sur les principes de la simulation, affichant les événements en temps réel et mettant en évidence l'importance personnelle de la cybersécurité pour les salariés. La plateforme met l'accent sur le développement des compétences et non uniquement sur la mise à disposition de connaissances. Chaque module comprend des exercices pratiques.

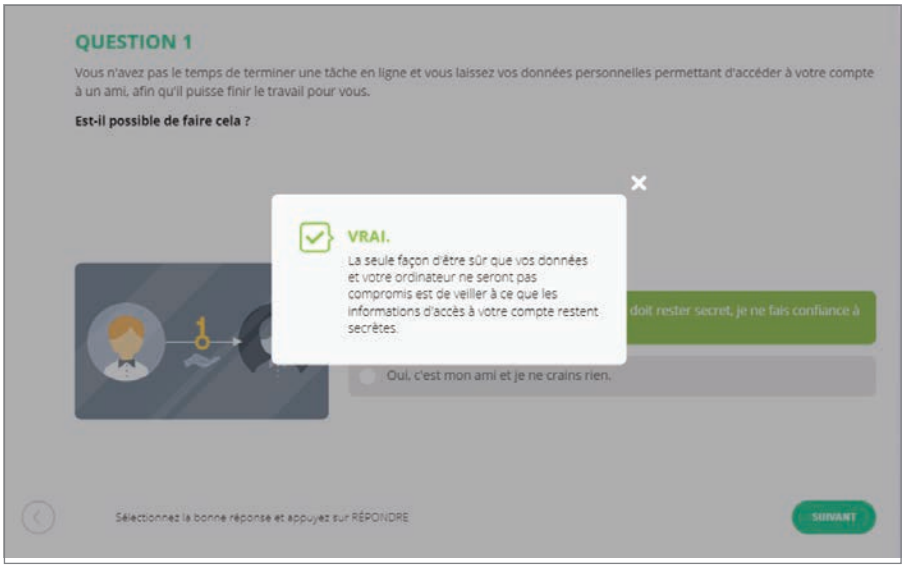
Les modules combinent différents types d'exercices pour que les utilisateurs restent intéressés et alertes, ainsi que pour les motiver à apprendre et à acquérir des comportements sûrs.

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







Jusqu'à 90 %

de réduction du nombre total d'incidents

Pas moins de 50 %

de réduction de l'impact financier des incidents

Jusqu'à 93 %

de probabilité que les connaissances soient appliquées dans le travail quotidien

Plus de 30x

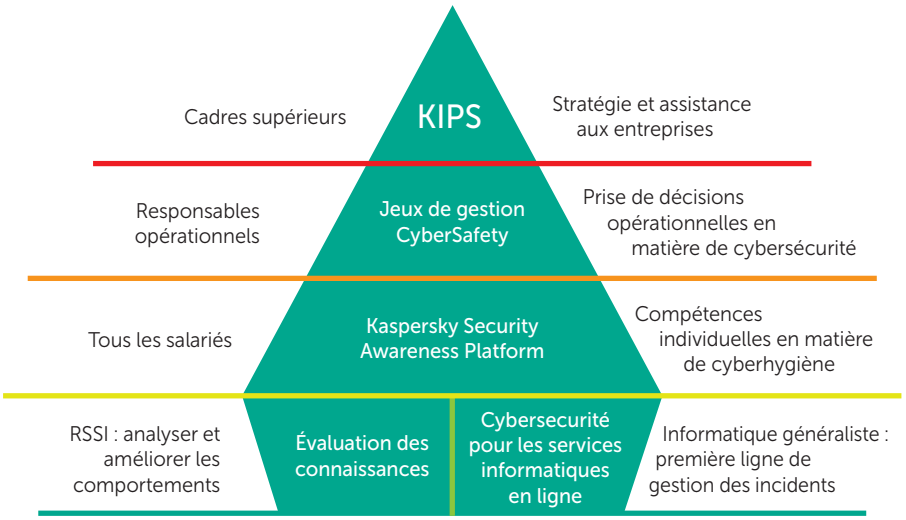
de retour sur investissement dans la sécurité

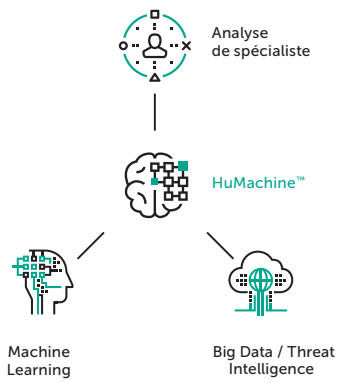
86 %

des participants, soit un pourcentage exceptionnel, sont prêts à recommander l'expérience

Kaspersky® Security Awareness

Automated Security Awareness Platform fait partie de la gamme de formations Kaspersky Security Awareness, qui propose des formations assistées par ordinateur ou en personne pour différents postes et niveaux organisationnels de votre entreprise.





Solutions de cybersécurité de Kaspersky Lab pour les entreprises :
https://www.kaspersky.fr/enterprise-security/security-awareness
Actualités des cybermenaces : www.viruslist.fr
Actualités de la sécurité informatique : business.kaspersky.com

https://www.kaspersky.fr/enterprise-security/security-awareness
#truecybersecurity
#HuMachine

www.kaspersky.fr