Solutions de cybersécurité de
Kaspersky Lab pour les entreprises

KASPERSKY lab

Plateforme de e-Learning

www.kaspersky.com/demo-sa
https://www.kaspersky.fr/enterprise-security/security-awareness
#truecybersecurity

Plateforme de e-Learning

Kaspersky Lab présente sa plate-forme de e-Learning dédiée aux employés, développée à partir du logiciel de formation primé de Wombat Security Technologies.

Il est important de s'appuyer sur des compétences et des connaissances. Aussi, l'accès à une plateforme de compétences en ligne est-il essentiel pour travailler sur des scénarios et des situations types, pour ensuite acquérir une meilleure compréhension des menaces potentielles et de la façon d'y faire face. L'apprentissage en ligne permet aux candidats de s'entraîner et d'apprendre par l'intermédiaire d'un portail interactif.

Aspects clés de la plateforme de e-Learning

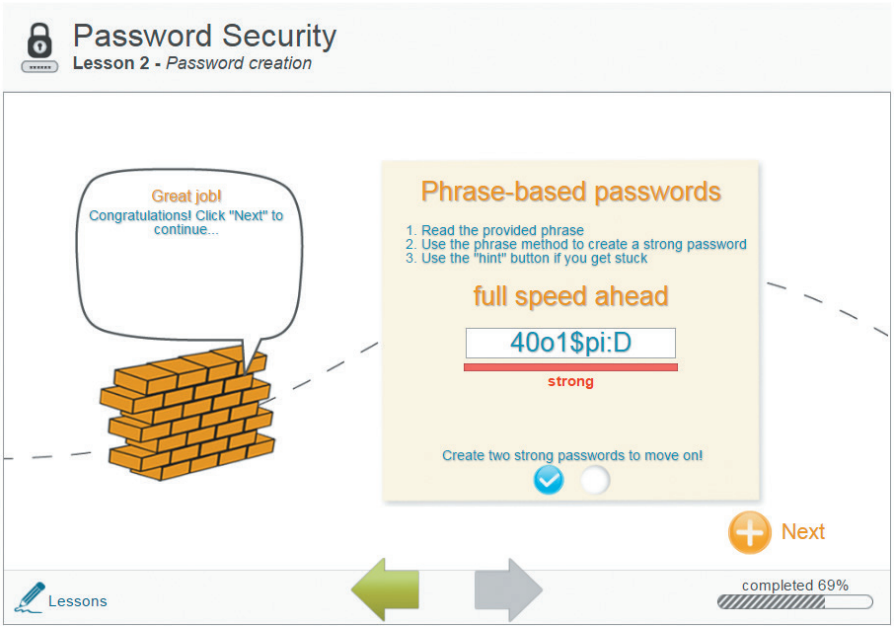
- **Modules de formation en ligne :** fondamentaux de la sécurité et fondamentaux de la sécurité pour les dirigeants, anti-phishing, protection et destruction des données, sécurité de la messagerie électronique, sécurité sur les réseaux sociaux, sécurité physique, sécurité des applications mobiles, sécurité des appareils mobiles, navigation sécurisée sur Internet, sécurité en dehors de l'entreprise ingénierie sociale, formation aux URL, mots de passe, informations d'identification personnelle (IIP), informations médicales protégées (IMP), paiements en ligne sécurisés (norme PCI DSS), protection contre les ransomwares, sécurité des appareils USB, sécurité lors des déplacements.

- **Évaluation des compétences :** pour déterminer en profondeur les compétences et les besoins en matière de formation de l'utilisateur. L'évaluation couvre divers domaines de sécurité et inclut des évaluations prédéfinies ou aléatoires et des questions définies par le client ; la durée est personnalisable.

- **Simulations d'attaques :** modèles personnalisables d'e-mails de phishing plus ou moins complexes et prêts à l'emploi. Lorsque le salarié reçoit un e-mail de phishing et clique dessus, il reçoit une alerte et se voit affecter automatiquement le module de formation pertinent.

- **Analyses et rapports :** résultats triés par campagne, groupe, type d'appareil, récidive, localisation.

Grâce à la plateforme, et au Guide des bonnes pratiques de Kaspersky Lab, le client sera en mesure d'établir et d'intégrer un plan de formation à la cybersécurité solide, continu et mesurable, en proposant à ses salariés des leçons simples au début et se compliquant progressivement par la suite, et en variant les domaines de sécurité en fonction des menaces et des compétences des salariés.



Évaluer

Évaluez les compétences de vos salariés et la vulnérabilité de votre entreprise grâce à nos évaluations et simulations personnalisables, identifiez les moments propices à l'enseignement et proposez des astuces et des conseils pratiques aux utilisateurs qui tombent dans le piège des fausses attaques USB, par phishing et par phishing SMS. Ces brefs exercices expliquent les dangers des attaques et contribuent à motiver les salariés à participer à la formation suivante.

Former

Faites votre choix dans un menu complet de modules de formation interactifs essentiels pour former vos salariés à la sécurité au travail et ailleurs. Ces modules de 10 à 15 minutes aident les utilisateurs à comprendre les risques potentiels, ainsi que la façon dont protéger les données personnelles et celles de l'entreprise.

Notre fonctionnalité d'auto-inscription vous permet d'affecter automatiquement une formation aux salariés qui se sont trompé lors d'un test de phishing ainsi qu'à ceux qui n'ont pas le niveau de maîtrise désiré lors d'évaluations CyberStrength® prédéfinies.

Renforcer

Rappelez à vos salariés les bonnes pratiques à adopter en leur envoyant des messages contenant des documents de sensibilisation conçus pour renforcer la formation et encourager l'assimilation des connaissances. Partagez des articles, affichez des posters, et récompensez les participants avec des cadeaux axés sur la sécurité.

Mesurer

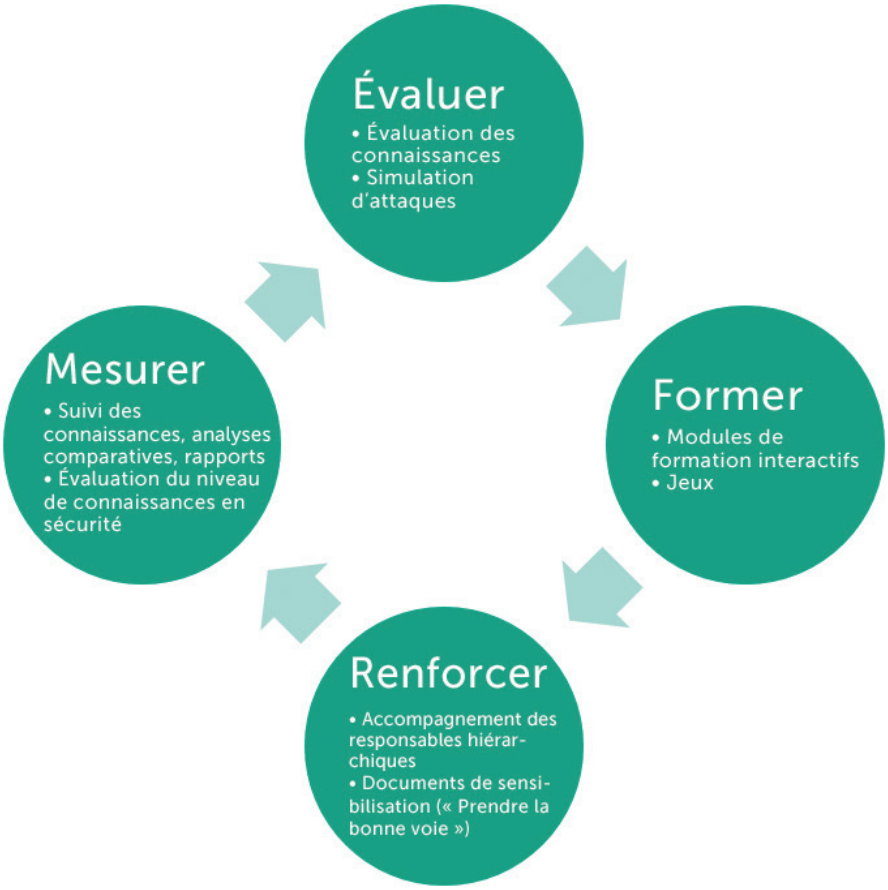
Recueillez des données d'analyse pertinentes sur les forces et les faiblesses de votre entreprise, évaluez les résultats et planifiez de futures formations en conséquence avant de répéter les quatre étapes du cycle.

Méthodologie

Nos clients en ont tiré avantage dans de nombreux secteurs, notamment un taux de réussite des attaques par phishing réduit (jusqu'à 90 %), une réduction des infections liées à des programmes malveillants (jusqu'à 95 %), des volumes d'appels à l'assistance technique réduits, un accroissement des signalements d'incidents par les salariés et une attitude en termes de sécurité généralement améliorée.

Ces résultats sont rendus possibles par l'intégration d'une méthodologie de formation continue à la sécurité et de solutions de formation sur la cybersécurité. Notre méthodologie de formation continue à la sécurité s'articule autour de quatre étapes clés : Évaluer, Former, Renforcer et Mesurer.

Ces composants peuvent être utilisés indépendamment, mais sont plus efficaces lorsqu'ils sont combinés, car ils proposent une approche à 360 ° de la sensibilisation et de la formation à la sécurité. Ces étapes sont disponibles via notre plate-forme de formation spécialement conçue pour les responsable de la sécurité IT et permettant une exécution sans faille de votre programme :



Avec nos solutions, les responsable de la sécurité peuvent facilement intégrer, gérer et surveiller les campagnes de formation, et mesurer leur succès grâce à des fonctionnalités de génération de rapports exhaustives. Au cours des premières étapes de cette méthodologie, responsables IT s'appuieront sur CyberStrength®, notre outil d'évaluation des connaissances, afin de connaître l'étendue des connaissances d'un utilisateur et de déterminer quels documents de sensibilisation seront nécessaires au développement du programme. Ils se serviront ensuite de simulations d'attaque afin d'évaluer la vulnérabilité des utilisateurs aux attaques et de les motiver à suivre la formation. Les données d'évaluation qui en résultent serviront à hiérarchiser les thèmes de formation les plus importants. Les e-modules de formation interactifs sur des thèmes sélectionnés seront ensuite affectés. Les progrès et le taux d'achèvement sont suivis.

Évaluations

- **Phishing Attacks** vous permet de créer des groupes, de concevoir une simulation d'attaque de phishing et de l'envoyer directement à vos utilisateurs. Si un utilisateur clique sur le lien, télécharge une pièce jointe ou saisit des informations sur une page d'accueil, il recevra un message d'alerte. Tous les utilisateurs qui se font piéger par cette attaque recevront un document leur montrant que leur action aurait pu être une erreur critique. Cela les rendra plus réceptifs et susceptibles de participer à une formation.
- **CyberStrength** vous permet de créer des évaluations des connaissances personnalisées afin de tester l'utilisateur final sur des thèmes liés à la cybersécurité.

Modules de formation interactifs

- **Fondamentaux de la sécurité** – Au cours de cette formation sur les fondamentaux de la cybersécurité, l'utilisateur sera confronté aux menaces et aux erreurs les plus courantes au quotidien.
- **Fondamentaux de la sécurité pour les dirigeants** – Grâce à cette formation, les dirigeants apprennent à reconnaître les menaces au travail comme à la maison, et à les éviter.
- **Formation aux URL** – Au cours de ce jeu interactif, les salariés apprennent à examiner une URL, à comprendre l'origine du lien et à identifier les URL malveillantes ou frauduleuses.
- **Sécurité de la messagerie électronique** – Au cours de ce jeu interactif, les utilisateurs apprennent à repérer des pièges de phishing et à reconnaître les pièces jointes, les informations et les liens contrefaits.
- **Anti-Phishing Phil** – Dans ce jeu mettant en scène un personnage, les salariés apprennent à examiner une URL, à comprendre l'origine du lien et à identifier les URL malveillantes ou frauduleuses.
- **Anti-Phishing Phyllis** – Dans ce jeu mettant en scène un personnage, les utilisateurs apprennent à repérer les pièges du phishing et à reconnaître les pièces jointes, les informations et les liens contrefaits.
- **Sécurité des mots de passe** – Les utilisateurs reçoivent des conseils et astuces pour créer des mots de passe plus forts, utiliser une famille de mots de passe simple à mémoriser et stocker leurs mots de passe en toute sécurité.
- **Sécurité sur les réseaux sociaux** – Formez vos utilisateurs sur les types d'« imposteurs » que l'on peut trouver en ligne, sur les dangers des réseaux sociaux et sur la manière de repérer les messages frauduleux qui y sont postés.
- **Protection contre les ransomwares** – Ce module de formation apprend à reconnaître et à prévenir les attaques par ransomwares.
- **Sécurité des appareils mobiles** – Apprenez à vos utilisateurs à sécuriser leur smartphone contre le vol, à créer des codes PIN, à maintenir la confidentialité de leurs communications et à éviter les applications dangereuses.
- **Sécurité des applications mobiles** – Apprenez à vos utilisateurs à rechercher des composants d'applications et expliquez-leur quelles sont les autorisations dangereuses, afin qu'ils puissent évaluer le degré de fiabilité et de sécurité d'une application mobile avant de la télécharger.
- **Sécurité des appareils USB** – Les utilisateurs finaux doivent prendre conscience des risques liés aux clés USB et autres éléments de l'IoT connectables aux ports USB, une menace souvent négligée.
- **Sécurité physique** – Apprenez à éviter et à corriger les failles de sécurité physique et prenez connaissance des bonnes pratiques à adopter pour protéger les personnes, les services et les ressources.
- **Sécurité au-delà du bureau** – Formez vos employés à l'utilisation sans risque du Wi-Fi gratuit, aux risques posés par les ordinateurs publics et aux moyens de préservation des équipements et des informations de l'entreprise, chez eux et en déplacement.
- **Navigation sécurisée sur Internet** – Les utilisateurs apprendront la différence entre le contenu d'un navigateur et le contenu d'un site Web, les moyens d'éviter les pop-ups malveillants dissimulant des virus, l'importance de la déconnexion sur les sites Web, les risques liés au remplissage automatique des formulaires et la manière de repérer les sites Web malveillants les plus courants.
- **Ingénierie sociale** – Les salariés apprendront à reconnaître les techniques courantes d'ingénierie sociale ainsi que les techniques pratiques à mettre en œuvre pour éviter les attaques, et découvriront comment pensent les escrocs adeptes de l'ingénierie sociale.
- **Informations d'identification personnelle (Personally Identifiable Information - IIP)** – Formez vos salariés aux différents types d'IIP, aux directives en matière d'identification, de collecte et de traitement des IIP, aux mesures à prendre en cas de violation d'IIP et aux astuces et techniques visant à améliorer la sécurité générale des IIP.
- **Norme sur la sécurité des données du secteur des cartes de paiement (*Payment Card Industry Data Security Standard*, « PCI DSS »)** – Les utilisateurs découvriront les contraintes de la PCI DSS, la conformité à cette norme, comment gérer des archives et des comptes, et comment reconnaître les violations de sécurité et agir en conséquence.

- **Protection et destruction des données** – Formez tout le monde aux différents types d'appareils électroniques portables et aux supports de stockage amovibles, aux avantages et inconvénients de chacun, aux bonnes pratiques de sécurisation des appareils et à l'élimination en toute sécurité des données.
- **Informations médicales protégées (IMP)** – (États-Unis uniquement) Cette formation interactive vise à former les salariés sur les exigences et les méthodes de sécurisation des IMP afin de répondre aux réglementations HIPAA, HITECH et Omnibus, notamment les bonnes pratiques à adopter pour l'utilisation, la divulgation, la transmission et le stockage des IMP.
- **Sécurité lors des déplacements** – Découvrez comment protéger vos données et vos appareils lorsque vous travaillez dans un aéroport, dans un hôtel, à une conférence et dans tout autre espace public.

Langues prises en charge

Configurations disponibles

Nos recommandations sur le choix de la configuration sont regroupées dans le tableau de comparaison détaillé ci-dessous :

1. Suite anti-phishing – Si votre souci principal est la réduction des attaques par phishing/programme malveillant.
2. Suite plurithématique – Si vous considérez le phishing comme un thème important, mais qu'une formation sur d'autres thèmes vous intéresse également (appareils/applications mobiles, protection des données, IIP/PCI, sécurité physique, mots de passe) et vous savez déjà quels thèmes sont les plus urgents/importants.
3. Plate-forme complète – Elle comprend tout ce qui précède, plus la capacité d'évaluer/comprendre les autres domaines de risques, afin de pouvoir cibler et hiérarchiser vos efforts de formation.

	Anti-phishing	Plurithématique	Complète
Simulations de phishing	Oui	Oui	Oui
Auto-inscription aux modules de formation	Oui	Oui	Oui
Affectation manuelle aux modules	–	Oui	Oui
CyberStrength (tests d'évaluation des connaissances)	–	–	Oui
Modules de formation inclus	3	Tous*	Tous*
Prise en charge des langues	Complète	Complète	Complète
Validité de la licence	1 an	1 an	1 an

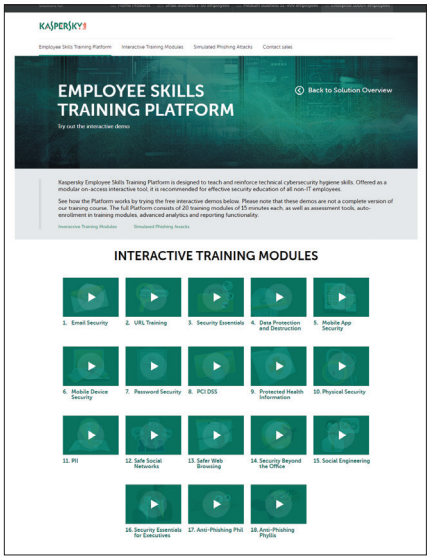
* « Tous » signifie tous les modules actuellement disponibles, ainsi que ceux disponibles à l'avenir

Testez la version démo de notre plate-forme !

www.kaspersky.com/demo-sa

Testez gratuitement la version démo interactive de nos modules de formation et de nos simulations d'attaques de phishing.

Pour en savoir plus (aspects administratifs, tarifaires, etc.), contactez votre responsable commercial Kaspersky Lab ou l'un de nos partenaires.



Démonstration

À des fins d'évaluation, et moyennant des frais distincts, Kaspersky Lab administrera pendant 30 jours un cycle de formation et d'évaluation anti-phishing comprenant un service de simulations d'attaques par phishing, un module « Formation aux URL » et un module « Sécurité de la messagerie électronique ». Ce projet se divise en 3 étapes :

- **Étape 1 : évaluation de la vulnérabilité aux attaques**
  Kaspersky Lab exécutera une campagne de simulations d'attaques par phishing afin d'établir une base de référence réaliste de la vulnérabilité de votre entreprise aux attaques déclenchées par notre service PhishGuru. Outre cette évaluation, les salariés recevront une formation au cours de laquelle ils apprendront à éviter les vulnérabilités futures.

- **Étape 2 : affectation des modules de formation anti-phishing**
  Kaspersky Lab affectera des modules de formation aux utilisateurs ayant échoué lors de la phase initiale de simulations d'attaques, tels que nos modules « Formation aux URL » et « Sécurité de la messagerie électronique ». L'affectation sera envoyée par e-mail aux utilisateurs s'étant fait prendre par les simulations d'attaque par phishing. Ces derniers auront un délai de 30 jours pour suivre les modules de formation.

- **Étape 3 : réévaluation de la vulnérabilité**
  À la fin de la période de 30 jours, Kaspersky Lab exécutera une deuxième campagne de simulations d'attaques par phishing à destination de l'ensemble des utilisateurs inclus dans l'attaque initiale de l'étape 1. Les résultats des deux campagnes seront analysés et un rapport final fourni au client.

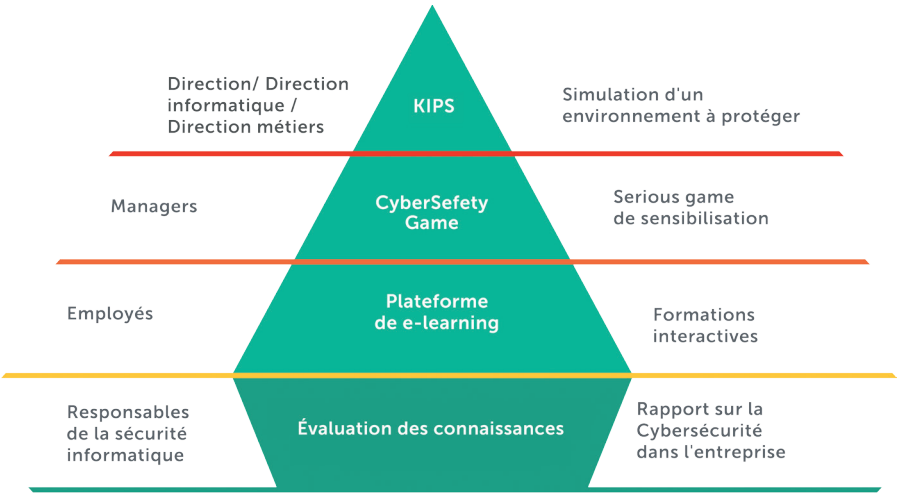
- **Responsabilité du client**
  Le client désignera un directeur de projet qui sera l'interlocuteur privilégié du chef de projet de Kaspersky Lab. L'interlocuteur fournira à Kaspersky Lab les informations et l'assistance nécessaires pour démontrer la faisabilité.

- **Éléments livrables**
  Nous fournirons un rapport final faisant état de la vulnérabilité et des améliorations à apporter.

Produits pédagogiques Kaspersky Security Awareness

La plate-forme de e-Learning dédiée aux salariés fait partie de la gamme Kaspersky Security Awareness, laquelle s'appuie sur une méthode prônant une culture de la cybersécurité. La culture de la cybersécurité est un ensemble de valeurs et d'attitudes influant sur le comportement des personnes, aussi bien au niveau individuel que de l'entreprise.

Nous aidons nos clients à développer une culture en cybersécurité, gérée par leurs équipes RH et de sécurité, par le biais de nos programmes de formation et de sensibilisation, présentés sous forme de jeu, et s'adressant à tous les niveaux de l'entreprise.



Une approche complète, mais simple

- Un large éventail de questions de sécurité couvert
- Des environnements familiers
- Un processus de formation axé sur la participation
- Des exercices pratiques
- Des explications compréhensibles par les néophytes

Avantages commerciaux

pas moins de

93 %

de chances de voir les salariés utiliser leurs connaissances au quotidien

jusqu'à

90 %

d'incidents en moins

50-60 %

de baisse des dépenses liées aux risques de cybersécurité

Multipl. par 30

du retour sur investissement en sensibilisation à la sécurité

www.kaspersky.fr

Solutions de sécurité Kaspersky Lab pour les entreprises :
https://www.kaspersky.fr/enterprise-security
Kaspersky Security Awareness :
https://www.kaspersky.fr/enterprise-security/security-awareness
Démonstration du produit : **www.kaspersky.com/demo-sa**