Solutions de cybersécurité de
Kaspersky Lab pour les entreprises

KASPERSKY lab

Jeux de plateau : sensibilisation à la cybersécurité

Formation immersive et motivante destinée aux managers pour promouvoir la prise de décisions en matière de cybersécurité

www.kaspersky.fr
#truecybersecurity

Jeux de plateau, de sensibilisation à la cybersécurité

Qui former ?

Les managers garants d'un environnement de travail sécurisé dans l'ensemble de l'entreprise

État général de la cybersécurité dans les entreprises (scénario correct) :

Entreprise

- Service de sécurité IT dédié
- Reconnaissance globale des problèmes
- Stratégie de cybersécurité optimale en place

Salariés

- Formation annuelle à la cybersécurité
- Fiches-conseils sur la cybersécurité dans certains bureaux

Toutes les entreprises tâchent de répondre aux cybermenaces en mettant en place des structures de sécurité IT et des programmes de formation conformes.
Mais est-ce suffisant ?

- Les connaissances que les salariés acquièrent dans le cadre des formations ont-elles réellement une influence sur leur comportement ? Ou la réponse est-elle ailleurs ?
- Faut-il sacrifier l'efficacité de l'entreprise pour atteindre un niveau de sécurité optimal ?
- Les responsable de la sécurité se sentent-ils en sous-effectif pour sensibiliser tout le monde à la cybersécurité ?

La seule solution face à ces défis est d'inciter les **managers à promouvoir une culture de la cybersécurité au sein de l'entreprise sans sacrifier l'efficacité de cette dernière. Ils sont les seuls** à interagir au quotidien avec les salariés et à prendre des décisions opérationnelles. Il s'agit d'intégrer les aspects de la cybersécurité à chaque prise de décision.

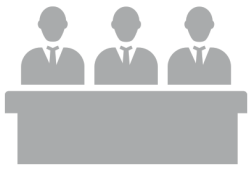
En règle générale, impliquer la direction est le principal défi de l'équipe de sécurité.

C'est la raison pour laquelle Kaspersky Lab a développé un programme de formation spécifique destiné à faire des responsables hiérarchiques / cadres les partisans et les ambassadeurs de la cybersécurité.

Rôle des cadres dans un environnement de cybersécurité bien réglé :

Entreprise

- Service de sécurité IT dédié et efficace en communication
- Stratégie de cybersécurité concrète
- Processus métier alignés sur les principes de cybersécurité



Managers

- Garants d'une utilisation efficace des principes de cybersécurité dans les tâches quotidiennes
- Assistance, surveillance et accompagnement des salariés

Salariés

- Formation continue à cybersécurité
- Évaluations régulières et efficaces avec adaptation automatique du parcours d'apprentissage

Résultats de la formation

Compétences nécessaires aux managers pour s'imposer comme ambassadeurs phares en matière de cyberhygiène

Grâce aux jeux de plateau de Kaspersky Lab, les responsables acquièrent **les connaissances, les compétences et les comportements** indispensables pour assurer la sécurité de leur environnement de travail au sein de leur service.

Compréhension

Adoption en interne de mesures de cybersécurité essentielles et à la fois très simples

Compétences acquises par les responsables :

- une prise de conscience quant à « la raison pour laquelle ils doivent se soucier de la sécurité »
- des éclaircissements sur la façon dont ils sont perçus par les cybercriminels
- une nouvelle compréhension des cybermenaces et des possibilités qui s'offrent à eux pour les éviter/prévenir

Contrôle

Perception du travail quotidien en gardant à l'esprit la cybersécurité

Compétences acquises par les responsables :

- la capacité à faire la distinction entre les comportements sûrs et dangereux
- la capacité à « analyser » au quotidien les lieux de travail habituels pour identifier les événements susceptibles de représenter une menace et sensibiliser les employés aux mesures de sécurité

Prise de décisions en matière de cybersécurité

Prise en compte de la cybersécurité comme partie intégrante des processus métier

Compétences acquises par les responsables :

- la capacité à trouver un équilibre optimal entre les précautions de sécurité et l'efficacité de l'entreprise
- la capacité à planifier et mettre en œuvre des projets tout en estimant le niveau de risques de cybersécurité à chaque étape et pour chaque équipe impliquée
- la capacité à évaluer le temps et le budget nécessaires pour prendre des décisions en matière de cybersécurité à chaque étape de chaque projet
- la capacité à coopérer efficacement avec l'équipe de sécurité

Les responsables ressortent convaincus qu'il n'est pas nécessaire que les mesures de sécurité soient complexes et chronophages pour éviter d'éventuelles pertes majeures de données personnelles et d'entreprise.

Renforcement et inspiration

Leadership d'influence et conseils utiles aux collaborateurs

Compétences acquises par les responsables :

- la capacité à répondre correctement aux questions des salariés en matière de cybersécurité ou à leur donner des conseils appropriés sur des sujets qu'ils ne maîtrisent pas totalement (par ex., en les redirigeant vers les experts de la sécurité IT ou en s'informant eux-mêmes)
- la capacité à maintenir un engagement continu envers les valeurs et les procédures de cybersécurité et à balayer toute forme de scepticisme à l'égard de ces valeurs
- la capacité à inciter le personnel à apprendre et appliquer activement au quotidien les techniques de cybersécurité
- enfin, un intérêt profond pour la cybersécurité, compatible avec les objectifs de l'entreprise, leurs propres objectifs et leur emploi du temps

10 domaines de sécurité sujets aux menaces :

Antivirus/applications, fuite de données, appareils mobiles, Web, messagerie électronique, comportement des victimes, ingénierie sociale, alertes de sécurité, vigilance, violation de politiques

Possibilité d'une « formation pour les formateurs »

Si un client souhaite utiliser les jeux de gestion de la cybersécurité pour former un plus grand nombre d'employés, de responsables et d'experts à travers divers services ou sites, il peut acheter une licence, former des formateurs internes et organiser des sessions de formation (sur site ou en ligne) à son propre rythme et selon ses propres besoins. Cette licence est disponible auprès de Kaspersky Lab et comprend :

- le droit d'utiliser en interne le programme de formation axé sur les jeux de gestion de la cybersécurité ;
- des supports de formation et le droit de les utiliser/reproduire ;
- des identifiants de connexion au serveur du logiciel de jeux de gestion de la cybersécurité ;
- un guide et une formation destinés aux formateurs, pour les responsables du programme ;
- un service de maintenance et d'assistance (mises à jour et assistance pour le logiciel et le contenu de formation) ;
- des options de personnalisation du scénario (moyennant un supplément).

Format du programme de formation

Programme attrayant de courtes formations sur ordinateur

Les jeux de gestion de la cybersécurité sont spécialement conçus pour s'adapter au mieux aux objectifs et aux priorités des responsables et pour les mettre à l'épreuve au moyen de simulations complexes et crédibles liées à l'environnement de travail.

Cette formation repose sur un **logiciel dédié aux jeux de plateau de sensibilisation à la cybersécurité** et couvre de façon ludique un éventail complet de thèmes relatifs à la sécurité. Le logiciel comprend des exemples, des explications et des exercices destinés à faciliter le travail du formateur.

De cette façon, la formation peut être dispensée par un formateur professionnel qui n'est pas nécessairement un expert en sécurité (le logiciel inclut l'intégralité des contenus relatifs à la sécurité).

Cette formation s'appuie sur l'hypothèse que les participants possèdent déjà quelques compétences techniques en matière de cybersécurité. Dans l'idéal, ils devraient avoir suivi plusieurs modules de la plate-forme de e-Learning dédiée aux employés de Kaspersky Lab. Si ce n'est pas le cas, il est possible de compléter les jeux de gestion de la cybersécurité avec une courte introduction théorique.

Programme de formation classique

Le programme de formation recommandé comprend trois modules qui s'accompagnent de brèves explications techniques et de réflexions sur les erreurs commises par les participants. Le client peut choisir d'ajouter ou de supprimer des modules.

Il est possible d'ajuster le programme et sa configuration en fonction de vos besoins particuliers (moyennant un supplément). Cependant, la plupart de nos clients sont satisfaits du programme classique dans la mesure où il couvre des environnements et des situations que toutes les entreprises et tous les responsables connaissent.

Session 1. « Il faut plutôt avoir peur des criminels, pas des ordinateurs endommagés par les virus »

2 heures

1. Identifier les cybermenaces – « Bureau ouvert »
2. Atténuation des risques :
   - Liens suspects et liens normaux
   - Mot de passe faible.
     Exercice : « Créer des mots de passe et des familles de mots de passe forts et mémorisables »
   - Pièces jointes suspectes et pièces jointes normales
   - Accès non autorisé à des informations confidentielles.
     Exercice : « Que faire pour atténuer les risques ? »
   - Diffusion inadéquate des informations confidentielles
   - Emporter des données confidentielles à l'extérieur de l'entreprise.
     Exercice : « Évaluer la situation commerciale et les risques associés »
   - Clé USB laissée sans surveillance.
     Exercice : « Que faire pour atténuer les risques ? »
   - Installer un logiciel non signé
   - E-mails de phishing.
     Exercice : « Comment repérer les e-mails frauduleux ? »
3. *Exercice : « Aperçu des criminels »*
4. Conclusion de la session
   - **N'oubliez pas :** « Il faut plutôt avoir peur des criminels, pas des ordinateurs endommagés par les virus »
   - **À faire :** « Toujours penser à qui pourrait faire mauvais usage de votre travail dans le monde numérique »

Session 2. « Il n'est pas nécessaire d'être une cible pour devenir une victime »

2 heures

1. Identifier les cybermenaces – *« En déplacement »*
2. Exercices d'atténuation des risques
   - Divulguer des e-mails – distinction entre messages personnels et professionnels
   - Ignorer les mises à jour de sécurité
   - Publications sur les réseaux sociaux – éviter les fuites d'informations
   - Partager un mot de passe.
     Exercice : « Évaluer la situation commerciale et les risques associés »
   - Installer une application sur un smartphone professionnel
   - PC déverrouillé.
     Exercice : « Que faire pour atténuer les risques ? »
   - Lien suspect.
     Exercice : « Formation aux URL suspectes »
   - Utiliser des informations confidentielles dans un lieu public
   - Authentification faible sur un réseau wifi public
3. Exercice : « Le profil de la victime »
4. Conclusion de la session
   - **N'oubliez pas :** « Il n'est pas nécessaire d'être une cible pour devenir une victime »
   - **À faire :** « Soyez plus difficile à cibler que les autres »

Session 3. « La cybersécurité est la responsabilité de chacun »

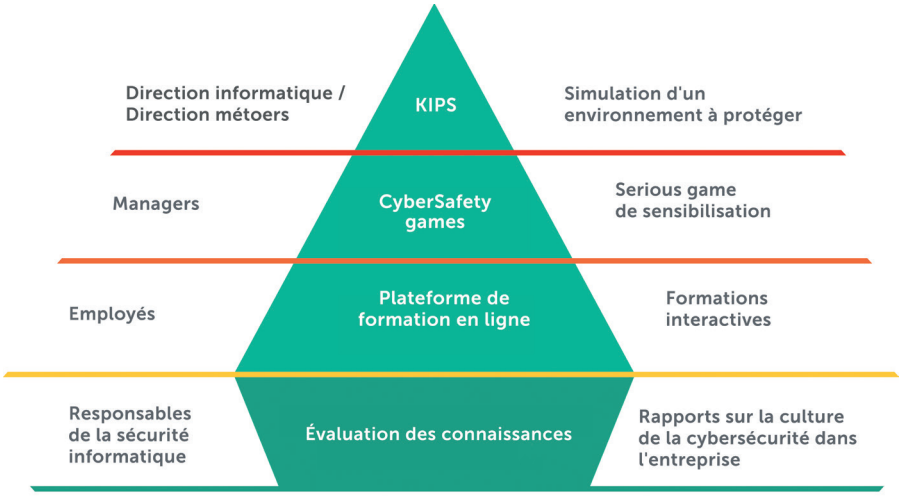
2 heures

1. Identifier les cybermenaces – « Salle de conférence »
2. Exercices d'atténuation des risques
   - Réutilisation et stockage des mots de passe
   - Divulgation accidentelle d'informations confidentielles.
     Exercice : « Que faire pour atténuer les risques ? »
   - Alertes DLP (Data Loss Prevention ou prévention des pertes de données)
   - Attaque d'ingénierie sociale.
     Exercice : « Comment reconnaître l'ingénierie sociale ? »
   - Ignorer la sécurité informatique
   - Envoyer des informations confidentielles à l'extérieur de l'entreprise.
     Exercice : « Évaluer la situation commerciale et les risques associés »
   - Sites Web malveillants
   - Emporter des données à l'extérieur de l'entreprise
   - Accès non autorisé à des informations confidentielles
   - Antivirus obsolète
   - Résoudre un objectif commercial avec des mesures de sécurité mises en place.
     Exercice : « Dialoguer avec le service de sécurité informatique »
3. *Exercice :* « Planifier la sécurité en tant que partie intégrante des activités »
4. Conclusion de la session
   - **N'oubliez pas :** « La cybersécurité est la responsabilité de chacun »
   - **À faire :** « Collaborer avec votre équipe de sécurité IT »

Produits pédagogiques Kaspersky Security Awareness

L'évaluation du niveau de connaissances en cybersécurité 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 :
www.kaspersky.fr/enterprise-security/security-awareness