



E4F

WOMEN IN GLOBAL EXPORT

e4f-network.eu

Liste des points de vigilance sur la cybersécurité dans le commerce électronique international.

La cybersécurité est un facteur essentiel à considérer dans le commerce électronique international. En effet, les transactions internationales de commerce électronique impliquent souvent le transfert transfrontalier de données sensibles, telles que des données financières et personnelles.

Pour assurer la sécurité de ces données, les organisations doivent utiliser diverses mesures de sécurité, comme le chiffrement, les passerelles de paiement sécurisées et l'authentification à deux facteurs.

En outre, les organisations devraient veiller à ce que leurs sites Web respectent les lois internationales en matière de protection de la vie privée et de sécurité des données.

Les organisations devraient surveiller leurs réseaux pour détecter toute activité suspecte et prendre les mesures appropriées pour se protéger contre les cybermenaces.

Cet outil est conçu pour indiquer aux utilisateurs si leur commerce électronique international comporte des mesures de protection de base contre les cyberattaques. Les grandes entreprises ont souvent des départements dédiés à ces fonctions, mais les petites entreprises ont souvent besoin de plus de ressources pour le faire.

Cet outil vous donnera un aperçu complet de la façon dont votre entreprise est protégée contre la cybercriminalité et peut-être identifier les lacunes ou les vulnérabilités qui peuvent être abordées.

Dans tous les cas, l'utilisateur prendra connaissance d'aspects de la cybersécurité qui n'ont peut-être pas été pris en compte et qui seront traités à temps, soit personnellement, soit par des professionnels spécialisés.



Co-funded by
the European Union

"Le soutien de la Commission européenne à la production de cette publication ne constitue pas une approbation du contenu qui reflète uniquement l'opinion des auteurs, et la Commission ne peut être tenue responsable de l'usage qui pourrait être fait des informations qu'elle contient."



E4F

WOMEN IN GLOBAL EXPORT

e4f-network.eu

L'outil est une liste de contrôle contenant des questions liées à la cybersécurité et au commerce électronique international. Pour chaque question, il y a trois réponses possibles selon l'expérience de l'utilisateur :

OUI :



NO:



Je ne sais pas :



Supposons que la plupart des réponses soient NON ou JE NE SAIS PAS. Dans ce cas, nous encourageons l'utilisateur à se mettre au travail pour améliorer la sécurité de son commerce électronique international afin d'éviter d'être victime d'attaques qui pourraient entraîner des pertes importantes ou même des échecs commerciaux.

Après la liste de contrôle, les utilisateurs trouveront une série de conseils pratiques sur la cybersécurité qui les guideront sur les prochaines étapes à suivre pour améliorer la sécurité en ligne de leur entreprise internationale.





E4F

WOMEN IN GLOBAL EXPORT

e4f-network.eu

LISTE DE VÉRIFICATION :

Questions



Votre site de commerce électronique est-il correctement crypté pour protéger les renseignements des clients pendant les transactions?

Avez-vous mis en œuvre des politiques de mot de passe strictes pour vos comptes clients et administratifs?

Mettez-vous régulièrement à jour les logiciels et les correctifs de sécurité de votre site Web pour vous protéger contre les vulnérabilités connues?

Avez-vous un plan en place pour intervenir en cas d'atteinte à la sécurité, comme un plan d'intervention en cas d'incident?

Tous les risques sont-ils pris en compte dans la stratégie de l'entreprise? Sinon, lequel ne l'est pas ?

Avez-vous formé vos employés aux pratiques exemplaires en matière de cybersécurité, comme la façon de repérer et de prévenir les attaques par hameçonnage?

Utilisez-vous des passerelles de paiement sécurisées et suivez-vous les protocoles de sécurité standard de l'industrie pour la manipulation et la transmission de renseignements sensibles sur les clients?

Avez-vous des mesures en place pour détecter et empêcher l'accès non autorisé aux données de votre site Web et de vos clients?

Avez-vous procédé régulièrement à des évaluations de sécurité et à des tests de pénétration pour cerner et corriger les vulnérabilités potentielles de votre système de commerce électronique ?



Co-financed by
the European Union

contenu qui reflète uniquement l'opinion des auteurs, et la Commission ne peut être tenue responsable de l'usage qui pourrait être fait des informations qu'elle contient."

du



E4F

WOMEN IN GLOBAL EXPORT

e4f-network.eu

Avez-vous des politiques et des procédures en place pour éliminer en toute sécurité les renseignements sensibles sur les clients lorsqu'ils ne sont plus nécessaires?

Avez-vous un processus pour surveiller et examiner régulièrement vos mesures de sécurité afin de vous assurer qu'elles demeurent efficaces?

Conseils sur la cybersécurité dans le commerce électronique international

1. Utilisez des réseaux sécurisés : assurez-vous d'utiliser des réseaux sécurisés, tels que les réseaux privés virtuels (VPN), pour protéger vos données lors de vos transactions en ligne.
2. Utilisez des mots de passe forts et uniques : Utilisez des mots de passe forts et uniques pour tous vos comptes en ligne et évitez d'utiliser le même mot de passe pour plusieurs comptes.
3. Activer l'authentification à deux facteurs : L'authentification à deux facteurs ajoute une couche de sécurité supplémentaire à vos comptes en ligne en vous demandant de saisir un code unique en plus de votre mot de passe.
4. Tenez les logiciels et les systèmes à jour : Mettez régulièrement à jour vos logiciels et vos systèmes pour vous assurer que vous disposez des derniers correctifs et fonctionnalités de sécurité.
5. Utilisez des méthodes de paiement sécurisées : Lorsque vous effectuez des transactions en ligne, utilisez des méthodes de paiement sécurisées, comme les paiements par carte de crédit cryptée ou les systèmes de paiement numériques comme PayPal.
6. Méfiez-vous des attaques d'hameçonnage : Méfiez-vous des attaques d'hameçonnage, qui sont des tentatives pour vous inciter à donner des informations sensibles, comme votre mot de passe ou les détails de votre carte de crédit.





E4F

WOMEN IN GLOBAL EXPORT

e4f-network.eu

7. Utilisez un logiciel de sécurité fiable : Utilisez un logiciel de sécurité fiable pour protéger vos appareils et vos données contre les logiciels malveillants et autres menaces.
8. Soyez prudent lorsque vous communiquez des renseignements personnels : Soyez prudent lorsque vous communiquez des renseignements personnels, comme votre nom, votre adresse et les renseignements de votre carte de crédit, en ligne. Ne partagez cette information qu'avec des sites Web et des commerçants de confiance.
9. Utiliser des canaux de communication sécurisés : Utilisez des canaux de communication sécurisés, tels que des applications de messagerie ou de messagerie cryptée, pour protéger vos informations sensibles tout en communiquant avec d'autres en ligne.
10. Surveiller les menaces et les atteintes potentielles à la sécurité et prendre des mesures immédiates au besoin.

En conclusion, la clé d'une cybersécurité efficace dans le commerce électronique international est d'avoir mis en place une stratégie de sécurité complète qui comprend divers outils et technologies pour se protéger contre les menaces potentielles.

Merci!



Co-funded by
the European Union

"Le soutien de la Commission européenne à la production de cette publication ne constitue pas une approbation du contenu qui reflète uniquement l'opinion des auteurs, et la Commission ne peut être tenue responsable de l'usage qui pourrait être fait des informations qu'elle contient."



E4F

WOMEN IN GLOBAL EXPORT

e4f-network.eu



E4F

WOMEN IN GLOBAL EXPORT



Co-funded by
the European Union

"Le soutien de la Commission européenne à la production de cette publication ne constitue pas une approbation du contenu qui reflète uniquement l'opinion des auteurs, et la Commission ne peut être tenue responsable de l'usage qui pourrait être fait des informations qu'elle contient."