Date de publication : 07/08/2024

Formation : Cybersécurité, sensibilisation des utilisateurs

Cours de synthèse - 1j - 7h00 - Réf. SES
Prix : 1010 CHF H.T.

4,4 / 5

BEST Blended

Ce cours vous permettra de connaître les risques et les conséquences d'une action utilisateur portant atteinte à la sécurité du système d'information, d'expliquer et de justifier les contraintes imposées par la politique de sécurité, comprendre les principales parades mises en place dans l'entreprise.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Comprendre la typologie de risques liés à la sécurité SI et les conséquences possibles
- Identifier les mesures de protection de l'information et de sécurisation de son poste de travail
- Favoriser la conduite de la politique de sécurité SI de l'entreprise

Public concerné

Tous les utilisateurs ayant accès au système d'information via un poste informatique.

Prérequis

Aucun.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

PARTICIPANTS

Tous les utilisateurs ayant accès au système d'information via un poste informatique.

PRÉREQUIS

Aucun.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

1 La sécurité informatique : comprendre les menaces et les risques

- Introduction : cadre général, qu'entend-on par sécurité informatique (menaces, risques, protection) ?
- Comment une négligence peut-elle créer une catastrophe ? Quelques exemples. La responsabilité.
- Les composantes d'un SI et leurs vulnérabilités. Systèmes d'exploitation client et serveur.
- Réseaux d'entreprise (locaux, site à site, accès par Internet).
- Réseaux sans fil et mobilité. Les applications à risques : web, messagerie…
- Base de données et système de fichiers. Menaces et risques.
- Sociologie des pirates. Réseaux souterrains. Motivations.
- Typologie des risques. La cybercriminalité en France. Vocabulaire (sniffing, spoofing, smurfing, hijacking...).

2 La protection de l'information et la sécurité du poste de travail

- Vocabulaire. Confidentialité, signature et intégrité. Comprendre les contraintes liées au chiffrement.
- Schéma général des éléments cryptographiques. Windows, Linux ou macOS : quel est le plus sûr ?
- Gestion des données sensibles. La problématique des ordinateurs portables.
- Quelle menace sur le poste client ? Comprendre ce qu'est un code malveillant.
- Comment gérer les failles de sécurité ? Le port USB. Le rôle du firewall client.

3 L'authentification de l'utilisateur et les accès depuis l'extérieur

- Contrôles d'accès : authentification et autorisation.
- Pourquoi l'authentification est-elle primordiale ?
- Le mot de passe traditionnel.
- Authentification par certificats et token.
- Accès distant via Internet. Comprendre les VPN.
- De l'intérêt de l'authentification renforcée.

4 Comment s'impliquer dans la sécurité du SI ?

- Analyse des risques, des vulnérabilités et des menaces.
- Les contraintes réglementaires et juridiques.
- Pourquoi mon organisme doit respecter ces exigences de sécurité ?
- Les hommes clés de la sécurité : comprendre le rôle du RSSI et du Risk manager.
- Agir pour une meilleure sécurité : les aspects sociaux et juridiques. La CNIL, la législation.
- La cybersurveillance et la protection de la vie privée.
- La charte d'utilisation des ressources informatiques.
- La sécurité au quotidien. Les bons réflexes. Conclusion.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque formation ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

Parcours certifiants associés

Pour aller plus loin et renforcer votre employabilité, découvrez les parcours certifiants qui contiennent cette formation :

- Parcours Assister les utilisateurs et transmettre les bonnes pratiques dans l'entreprise - Réf. ZTM
- Parcours Assister les utilisateurs et transmettre les bonnes pratiques dans l'entreprise - Réf. ZTM

Options

Blended : 105 € HT

Approfondissez les connaissances acquises en formation grâce aux modules e-learning de notre Chaîne e-learning culture digitale. Un apprentissage flexible et complet, à suivre à votre rythme dès le premier jour de votre présentiel.

Dates et lieux

CLASSE À DISTANCE

2026 : 11 juin, 11 juin, 24 sep., 24 sep., 3 déc., 3 déc.