

Cybersécurité, sensibilisation des utilisateurs

DESCRIPTION :

- 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 justifier les contraintes imposées par la politique de sécurité, comprendre les principales parades mises en place dans l'entreprise.

DURÉE :

- 1 Journée - 7h.

PRÉ-REQUIS :

- Aucune connaissance particulière

OBJECTIFS :

- 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 :

- Tous les utilisateurs ayant accès au Système d'Information via un poste informatique.

ACCESSIBILITÉ :

- L'accessibilité au centre de formation ACKWARE, permet aux personnes handicapées de circuler avec la plus grande autonomie possible, d'accéder aux locaux et équipements, d'utiliser les équipements et les prestations, de se repérer et de communiquer. L'accès concerne tout type de handicap (moteur, visuel, auditif, mental...).

ANIMATION : PRESENTIEL OU CLASSES À DISTANCE

CLASSES À DISTANCE :

- A l'aide d'un logiciel comme Teams, Skype, Zoom etc...un micro et éventuellement une caméra pour l'apprenant.
- Suivez une formation en temps réel et entièrement à distance. Lors de la classe en ligne les apprenants interagissent et communiquent entre eux et avec le formateur.
- Les classes à distance sont organisées en Inter-Entreprises comme en Intra-Entreprise.

MÉTHODES PÉDAGOGIQUES :- Développement Personnel - Santé

- Réflexions de groupe et apports théoriques du formateur
- Travail d'échange avec les participants sous la forme de brainstorming
- Auto diagnostic du stagiaire : Bilan des points forts et repérage des points faibles.
- Utilisation de cas concrets issus de l'expérience professionnelle
- Validation des acquis par des questionnaires, des tests d'évaluations, des mises en situation et des jeux pédagogiques.
- Remise d'un support pédagogique

SUIVI ET EVALUATION

- Evaluation de la formation par les participants et remise d'une certification ou d'une attestation de fin de formation à chaque apprenant.



ACKWARE VOUS ACCOMPAGNE DANS TOUS VOS PROJETS DE FORMATION ET VOUS APPORTE SON EXPERTISE POUR VOTRE TOTALE SATISFACTION



Cybersécurité, sensibilisation des utilisateurs

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...).

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 MAC OS : 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.

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.

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.