Le 08/07/2024

Sensibilisation à la Cyber Sécurité

Durée : 0,5 jour soit 4 heures

Objectifs **:** **Comprendre les enjeux et être sensibiliser à la Cybersécurité et à la Cyberdéfense**
L'apprenant sera capable de :
- Identifier les menaces courantes
- Assurer la maintenance des sécurités de base des systèmes informatiques
- Naviguer de manière sécurisée
- Réagir en cas d'incident

Prérequis **:** Aucun

Réalisation : Présentiel

Date(s) et lieu **:** A définir

Public **:** Dirigeants et Comité de Direction

Accessibilité : Pour les personnes atteintes d'un handicap, nous contacter

Débouchés Tous métiers

Contact **:** Edwige CILIONE, formatrice bureautique expérimentée depuis 25 ans et entourée d'une équipe de formateurs professionnels

Modalités d'accès **:** A la signature de la convention et/ou de la prise en charge

Délai d'accès : De 2 jours à 4 semaines

Type action **:** Actions d'acquisition, d'entretien ou de perfectionnement des connaissances

Méthode pédagogique : Méthode active, démonstrative et participative
Exercices autonomes réguliers pour s'assurer de l'assimilation

Méthode d'évaluation **:**
1. des acquis :
Evaluation de l'atteinte des objectifs par grille critériée
2. à chaud :
Questionnaire évaluation de formation pour mesurer le niveau de satisfaction

Tarif : 1 290 € net de taxes
Exonéré de TVA

Siège social : 10 rue du Bordeau - 89100 ST DENIS - www.form-info.fr - Tél.: 06.83.24.25.34 - ✉ edwige.cilione@form-info.fr
Déclaration d'activité enregistrée sous le numéro N° 26 89 01244 89 auprès du préfet de la région Bourgogne

Le 08/07/2024

Sensibilisation à la Cyber Sécurité

CONTENU DU MODULE

La sensibilisation des dirigeants à la cybersécurité nécessite une approche pédagogique spécifique qui tient compte de leur niveau d'expertise, de leur emploi du temps chargé et de leur responsabilité dans la protection de l'entreprise.

1. **Les types de cybermenaces** : Comprendre les différentes formes de cyberattaques auxquelles une entreprise peut être confrontée, telles que les attaques par phishing, les ransomwares, les attaques par déni de service (DDoS), etc. Cela permet au dirigeant d'identifier les vulnérabilités potentielles de son entreprise et de prendre des mesures pour les atténuer.
2. **Les conséquences des cyberattaques** : Connaître les conséquences financières, juridiques et réputationnelles des cyberattaques sur une entreprise. Cela inclut les pertes financières directes, les amendes réglementaires, les litiges, ainsi que la perte de confiance des clients et des partenaires commerciaux.
3. **La réglementation en matière de cybersécurité** : Être conscient des lois et des réglementations nationales et internationales en matière de protection des données et de cybersécurité, telles que le RGPD (Règlement Général sur la Protection des Données) en Europe. Comprendre les exigences réglementaires permet au dirigeant de garantir que son entreprise est en conformité et évite les sanctions potentielles. Tel que les déclaration CNIL en cas de défaillance.
4. **La gestion des risques** : Avoir une compréhension approfondie de la gestion des risques liés à la cybersécurité, y compris l'identification des menaces, l'évaluation des vulnérabilités et la mise en place de mesures de protection appropriées. Cela permet au dirigeant de prendre des décisions stratégiques pour atténuer les risques et protéger les actifs numériques de l'entreprise.
5. **La culture de sécurité** : Reconnaître l'importance de promouvoir une culture de sécurité au sein de l'entreprise, où la sécurité informatique est une priorité pour tous les employés, du haut niveau à la base. Encourager la sensibilisation, la formation et l'adoption de bonnes pratiques de sécurité contribue à renforcer la posture de sécurité globale de l'entreprise.
6. **L'investissement dans la cybersécurité** : Comprendre que la cybersécurité nécessite un investissement continu en termes de technologies, de ressources humaines et de formation. Reconnaître l'importance d'allouer des ressources adéquates à la cybersécurité pour garantir la protection des actifs numériques de l'entreprise.
7. **Définir le plan d'action approprié :** Le dirigeant et comité de direction seront mieux équipés pour prendre des décisions stratégiques et mettre en œuvre les mesures efficaces pour protéger son entreprise contre les cybermenaces et sensibiliser ses employés.

L'apprenant pourra, par la suite, suivre une formation correspondant au niveau suivant.
Le nombre de participants est de **5 maximum** par stage.
Un support et les documents de cours sont remis à chaque participant.
Chaque stagiaire dispose d'un micro-ordinateur.
L'apprentissage est basé sur des exercices pratiques entre chaque module de cours.

Siège social : 10 rue du Bordeau - 89100 ST DENIS - www.form-info.fr - Tél.: 06.83.24.25.34 - ✉ edwige.cilione@form-info.fr
Déclaration d'activité enregistrée sous le numéro N° 26 89 01244 89 auprès du préfet de la région Bourgogne