GC12 – SENSIBILISATION CYBERSECURITE

Objectifs

Utiliser les fonctionnalités courantes et avancées de la gestion commerciale en toute autonomie. Utiliser les fonctionnalités courantes et avancées de la comptabilité en autonomie au quotidien.

Public visé

Tous le monde

Prérequis :
Connaissances des processus opérationnels de la pme
Disposer d'un pc portable avec un navigateur Web et d'une connexion internet.

Méthodes et outils pédagogiques :

Cours en groupe de 4 à 5 personnes
Cours théoriques, exposés et échanges de questions/réponses
Démonstration, saisie et utilisation dans le logiciel métier

Modalités d'évaluation formalisées des objectifs de la formation :

Quizz en fin de formation permettant d'évaluer les acquis du stagiaire
Certificat de réalisation

Formateur Nicolas Mariage Formateur Cybersécurité

Lieu : Sur site, chez le client ou dans une salle externe. Si vous êtes en situation de handicap, nous sommes à votre écoute et mettons en œuvre les mesures nécessaires afin de vous accompagner et faciliter votre accessibilité à cette formation (cf. contact commercial).

Durée : 1 jour (7 heures)

Modalités et délais d'accès à la formation :

Variables en fonction du statut, du financeur et du planning de nos formations, merci de nous contacter.

Tarif : 900 € HT / la journée

Contact : formation@mohatra.fr

ELEMENTS DE CONTENU :

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, phishing, arnaque au président, 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 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.

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.