CYBERPROTECTION (CYBER)

GESTIC FORMATION
Formation Professionnelle • Logiciel • Solution Informatique

Prérequis

> Savoir utiliser un ordinateur (basique).
> Savoir naviguer sur Internet (basique).

Objectifs

> Comprendre ce qu'est la cybercriminalité.
> Identifier les risques informatiques.
> Identifier les risques potentiels malveillants en interne et en externe de la société.
> Être capable de remonter une faille de sécurité.
> Être réactif par rapport à une attaque informatique.
> Être force de proposition en matière de sécurité informatique.
> Anticiper un risque informatique.
> Pouvoir suivre la sécurité mise en œuvre par un prestataire informatique.
> Savoir mieux maîtriser son système d'information.

Modalités d'évaluation

> Un questionnaire initial pour les apprenants pour tester leurs connaissances.
> Des questionnaires au fil de l'eau des thématiques abordées.
> Un questionnaire final pour évaluer les nouvelles connaissances des apprenants.

Public

> Salarié, non salarié, gérant, gérant non salarié, artisan, demandeur d'emploi.

Compétences

> Utilisation de l'outil informatique (ordinateur, tablette, smartphone).
> Sensibilité aux nouvelles technologies numériques.

Qualités - Aptitudes

> Assiduité.
> Autonomie.
> Écoute.
> Pertinence.

Délai d'accès

> Selon le calendrier en cours - Merci de prendre contact avec notre service.

Durée

> 1 jour soit 7 heures.

Tarif

> 790€HT/jour soit 948€TTC/jour en intra-entreprise - Nous consulter.

Lieu

> En nos locaux à Biard. Possibilités en vos locaux sous conditions - nous contacter.

Méthodes mobilisées

> 100% face à face pédagogique.
> Notre pédagogie est basée sur la mise en pratique de cas professionnels avec alternance d'apports théoriques et de mise en pratique informatique tout au long des modules afin de valider les acquis.
> Des démonstrations techniques pourront être réalisées.
> Des présentations et des cas concrets seront explicités, analysés pour une meilleure compréhension des risques et permettront d'expliquer comment mettre en place des parades.
> Les stagiaires disposeront en fin de séance d'un support en trois parties « bons réflexes » permettant de sécuriser l'entreprise le soir à la fermeture des bureaux.
> Chaque stagiaire travail sur un PC.
> Intra-Entreprise ou Inter-Entreprises.
> 100% Présentiel ou distanciel (visio) - Nous contacter.

Contenu

> Ciblage des environnements régulièrement attaqués.
> Les systèmes d'information (SI) et les failles les plus souvent rencontrées.
> L'humain au centre des attaques informatiques.
> Quels sont les enjeux liés à la sûreté pour une entreprise ou un particulier.
> Quelles sont les définitions des principales attaques des hackers.
> Quelles sont les mesures adaptées à chaque attaque.
> Comment sécuriser le télétravail.
> Parmi l'ensemble des thèmes abordés sont inclus : Les FOVI; le WIFI; le typosquatting; l'IA; les smartphones; les BYOD; les CB; les Rançongiciels.

Votre contact

> **Marina Laurent** - Assistante Administrative et Commerciale : **m.laurent@gestic-formation.com 05 49 52 55 04**

Accessibilité

> Nos locaux sont accessibles au public en situation de handicap.
> Centre Handi-Accueillant.
> **Amélie Bertin** - Référente Handicap : **a.bertin@gestic-formation.com**

« Selon le rythme de pratique, il faut de 1 à 3 mois pour acquérir solidement le contenu d'un déroulé pédagogique »

Gestic Formation - 1 Rue de la Tardiverie - ZAE Larnay - 86580 Biard- Tél. : 05 49 52 55 04 - Mail : info@gestic-formation.com