Handle a Good Business

COMPÉTENCES ESSENTIELLES

PROGRAMME DE FORMATION

CYBERSECURITE ET PROTECTION DES DONNEES - NIVEAU I

1. OBJECTIFS

Il s'agit d'une action de formation individuelle (intra-entreprise).

La formation WordPress permet aux porteurs de projet de :

- Identifier les menaces numériques courantes et adopter des pratiques de prévention adaptées
- Sécuriser leurs appareils, mots de passe, e-mails et réseaux Wi-Fi pour protéger leurs données
- Appliquer des bonnes pratiques pour naviguer sur Internet et gérer les données sensibles
- Réagir efficacement face à des cyberattaques en suivant des étapes d'urgence claires
- Comprendre et respecter les régulations comme le RGPD pour garantir la conformité légale

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

- Reconnaître et éviter les principales menaces de cybersécurité (phishing, malware, etc.)
- Créer et gérer des mots de passe robustes et sécurisés,
- Appliquer des pratiques sécurisées pour naviguer et utiliser des services en ligne
- Identifier et sécuriser les données personnelles et sensibles,
- Protéger ses appareils et réseaux grâce à des outils adaptés (VPN, antivirus, etc.)
- Réagir efficacement face à une cyberattaque ou une compromission de données
- Connaître les bases du RGPD et des droits sur les données personnelles

2. NIVEAU DE CONNAISSANCE PRÉALABLE REQUIS - PUBLIC CIBLE

Les stagiaires doivent avoir une expérience dans le domaine du numérique, mais pas de connaissances spécifiques en Cybersécurité et Protection des données.

3. PROGRAMME DE FORMATION

Le programme se déroule sur 4 jours : 05, 06 décembre 2024 et 08, 09 janvier 2025

JOUR 1 - Introduction et concepts fondamentaux de la cybersécurité

INTRODUCTION À LA CYBERSÉCURITÉ

→ Définition et importance de la cybersécurité
→ Principales menaces informatiques (malware, phishing, ransomware, etc.)
→ Cas d'exemples récents d'attaques

SÉCURITÉ DES MOTS DE PASSE

→ Règles pour créer un mot de passe fort et sécurisé
→ Outils de gestion de mots de passe (présentation et démonstration)
→ Exercices pratiques sur la création de mots de passe robustes

PHISHING ET INGÉNIERIE SOCIALE

→ Qu'est-ce que le phishing et comment le reconnaître ?
→ Autres techniques d'ingénierie sociale utilisées par les attaquants
→ Études de cas et exemples pratiques
→ Simulation de phishing pour comprendre les impacts

SÉCURISATION DES APPAREILS PERSONNELS ET PROFESSIONNELS

→ Bonnes pratiques pour la navigation sur Internet
→ Antivirus et autres logiciels de protection

JOUR 2 - Bonnes pratiques et sécurité avancée

GESTION DES E-MAILS ET SÉCURITÉ NUMÉRIQUE

→ Recommandations pour éviter les e-mails frauduleux
→ Bonnes pratiques pour sécuriser sa boîte mail
→ Exercices interactifs sur la détection de spams et de faux messages

SÉCURISATION DES RÉSEAUX WI-FI

→ Présentation de VPN et leur utilisation

PROTECTION DES DONNÉES SENSIBLES

→ Qu'est-ce que la protection des données personnelles (RGPD et autres régulations) ?
→ Bonnes pratiques pour le stockage sécurisé des données

RÉAGIR FACE À UNE CYBERATTAQUE

→ Étapes à suivre en cas de suspicion de compromission
→ Contacter le service informatique et les autorités compétentes
→ Les premiers gestes pour limiter l'impact

JOUR 3

COMPRENDRE CE QUE SONT LES DONNÉES PERSONNELLES

→ Définition et exemples de données personnelles et sensibles
→ Importance de la protection des données dans la vie quotidienne
→ Historique et exemples d'incidents de fuite de données

BONNES PRATIQUES DE PROTECTION DES DONNÉES

→ Comment créer et gérer des mots de passe sécurisés
→ L'importance de verrouiller ses appareils (ordinateur, téléphone)
→ Reconnaître les tentatives de phishing et d'escroqueries en ligne

SENSIBILISATION À LA SÉCURITÉ SUR INTERNET

→ Naviguer en toute sécurité : conseils sur l'utilisation des sites web sécurisés (HTTPS)
→ Télécharger de manière sûre : éviter les logiciels et fichiers douteux
→ Exercices simples de détection de risques sur des sites web fictifs

STOCKAGE ET PARTAGE DE DONNÉES

→ Stocker les données sur des supports sécurisés (ex. : disque dur, cloud sécurisé)
→ Conseils sur le partage de fichiers et l'envoi d'e-mails de manière sécurisée

JOUR 4

UTILISATION DE LOGICIELS DE BASE POUR LA PROTECTION DES DONNÉES

→ Introduction aux gestionnaires de mots de passe gratuits et faciles à utiliser

→ Présentation des options simples de sauvegarde des données (cloud sécurisé)

APPRENDRE À SÉCURISER LES APPAREILS

→ Vérifications de base : mises à jour des logiciels et activation des pare-feux

→ Paramètres de confidentialité sur les réseaux sociaux et applications mobiles

INTRODUCTION AUX RÈGLES DE BASE DU RGPD

→ Ce que le grand public doit savoir sur le RGPD et les droits sur leurs données personnelles

→ Exercices pratiques : comprendre et gérer ses propres paramètres de confidentialité sur les sites web

PLAN D'ACTION PERSONNEL POUR LA PROTECTION DES DONNÉES

→ Check-list simple de bonnes pratiques à adopter au quotidien
→ Rédaction d'un plan d'actions personnelles pour sécuriser ses données

4. LE SUIVI DE LA REALISATION DE L'ACTION

S'agissant d'une formation individuelle, elle se déroule dans les locaux de la société.

Un seul formateur assure la formation. Il dispose de son propre ordinateur portable et fournit la documentation nécessaire durant la formation. Pendant la session, le stagiaire reçoit des feuillets d'exercices à réaliser en séance ; la reprographie est assurée par le formateur.

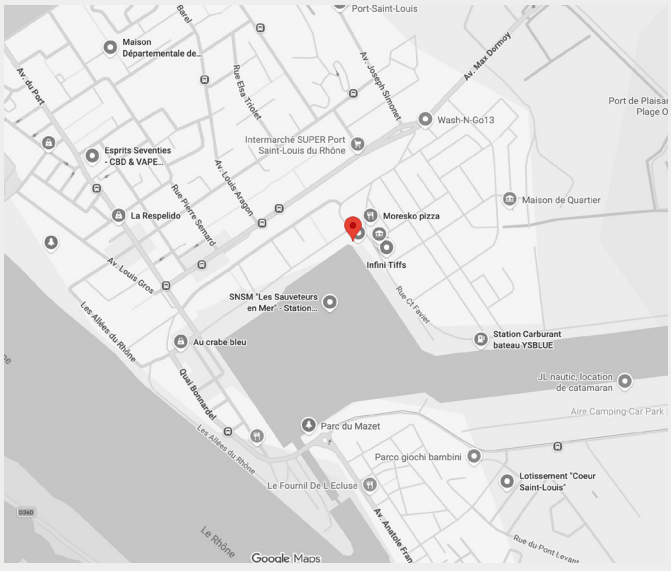
5. LE SUIVI DE LA REALISATION DE L'ACTION

Les feuilles d'émargement sont signées par le stagiaire et le formateur (comportant la date, la durée, l'intitulé de l'action). Ces feuilles d'émargement permettent l'établissement des attestations de présence par le commanditaire de la formation.

6. LES MOYENS D'EVALUATION MIS EN OEUVRE

Une fiche d'appréciation est remise par le formateur au stagiaire en fin de stage, afin de recueillir ses observations, remarques et critiques.Il s'appuie sur ces éléments pour faire le bilan des connaissances acquises et déterminer la nécessité de prolonger ou reconduire l'action de formation.

Un suivi des questions de la part du stagiaire est assuré avec HGB grâce à des échanges réguliers par voie électronique.



Handle a Good Business

LIEUX DE LA FORMATION

Rue du Commandant Favier
13230 Port-Saint-Louis-du-Rhône

CONTACT

04 42 93 73 81