

PROGRAMME DE FORMATION | CYBERSECURITE PARCOURS INTRODUCTIF

Réf. : FRM-CYBINTRO

Durée : 3 jours, soit 21 heures

Public visé : Cette formation est adaptée à toute personne ayant un intérêt pour les réseaux informatiques.

Prérequis : Avoir des connaissances de base en informatique et en réseaux, ainsi qu'une compréhension des systèmes d'exploitation et des équipements réseau.

Objectifs pédagogiques : À l'issue de l'introduction à la Cybersécurité, les participants seront sensibilisés aux risques courants liés à la cybersécurité dans leur usage quotidien de l'informatique ; de fournir des compétences pratiques pour se protéger contre les menaces en ligne, telles que le phishing, les logiciels malveillants et les violations de données.

Délai d'accès : Précisé à la demande, selon vos disponibilités et celles de la personne en charge de la formation.

Contenu

1. Sensibilisation aux menaces et à la cybersécurité de base

1.1. Initiation à la cybersécurité

- Comprendre les enjeux de la sécurité des systèmes d'information : les enjeux, pourquoi les pirates s'intéressent-ils au SI, la nouvelle économie de la cybersécurité
- Connaitre les besoins de sécurité, les notions de base et vocabulaire
- Voir un panorama de quelques menaces

*Exemples de cas pratiques :
Exemples d'attaques connues et leurs modes opératoires*

2. Les bases de la sécurité numérique

- Détecter des tentatives d'hameçonnage
- Identifier des courriels indésirables ou dangereux
- Naviguer sur Internet en toute sécurité
- Maîtriser des données personnelles et des informations de navigation
- Générer des mots de passe robustes
- Prendre les précautions relatives à la sécurité

*Exemples de cas pratiques :
Prise en main des bonnes pratiques de la base de cybersécurité.*

3. Sécurisation des outils numériques et des données

- Sécuriser des équipements informatiques
- Protéger des données personnelles et professionnelles
- Utiliser de manière sécurisée les réseaux
- Sécuriser sur les réseaux sociaux et les plateformes en ligne

*Exemples de cas pratiques :
Prise en main de sécurisation des données*

4. Gestion des incidents et diffusion des bonnes pratiques

- Réagir face aux incidents de cybersécurité
- Diffuser les bonnes pratiques en cybersécurité
- Atelier pratique : Simulation d'incident et retour d'expérience

*Exemples de cas pratiques :
Mise en pratique d'une situation de sécurisation des données de la création à l'utilisation en distanciel*

PROGRAMME DE FORMATION | CYBERSECURITE PARCOURS INTRODUCTIF

Méthode pédagogique

Formation intra-entreprise délivrée en présentiel ou distanciel, personnalisée aux besoins spécifiques des stagiaires, en groupe avec un formateur spécialiste des matières abordées.

Méthodes pédagogiques actives et participatives. Alternance de théorie et de pratique avec application au contexte des participants. Le formateur alterne entre méthode démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Les stagiaires appréhenderont les fondamentaux et les particularités du logiciel Arduino afin de le comprendre et ainsi de gérer de façon autonome et grâce au logiciel, le développement de leur propre programme à l'aide des travaux pratiques prévus par le formateur.

Moyens et supports pédagogiques

La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions.
Variables suivant les formations, les moyens pédagogiques mis en œuvre sont :

- Ordinateurs, connexion internet, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

Dans le cas d'une formation sur site Entreprise, le client s'assure et s'engage à avoir toutes les ressources pédagogiques nécessaires (salle, équipements, accès internet, TV ou Paperboard...) au bon déroulement de l'action de formation conformément aux prérequis indiqués dans le programme de formation

Modalités d'évaluation et de suivi

Le formateur évalue la progression pédagogique des stagiaires tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques... Les participants complètent également un test de positionnement en amont et en aval pour valider les compétences acquises.

L'émargement des stagiaires et du formateur est réalisé chaque demi-journée afin d'assurer le suivi de l'assiduité.

Un questionnaire de satisfaction à chaud et à froid est proposé à l'issue de la formation pour mesurer la perception et l'impact de la formation.