Guiddy

Programme de formation

Formation à la Cybersécurité

(Formation accessible aux personnes en situation de handicap)

I. Personnes visées

- Toutes personnes de l'entreprise utilisant un outil du SI

II. Prérequis

- Aucun

III. Durée

- 1 jour (7h)

IV. Lieu et horaire

- En intra
- Les cours ont lieu de 9h à 12h30 et de 14h à 17h30

V. Délai d'accès aux formations

- Nos formations sont sur mesure et les dates et horaires adaptés aux besoins

VI. Nombre de participants

- 3 à 10 personnes

VII. Tarif

- Nous contacter : 06.33.37.90.91 / contact@guiddy.fr

VIII. Objectifs de la formation

- Prendre conscience des enjeux et des risques relatifs à la cybersécurité
- Connaître les acteurs et les ressources de la cybersécurité
- Identifier les menaces potentielles et savoir réagir
- Mettre en œuvre les bonnes pratiques pour se prémunir des risques liés à la sécurité des systèmes d'information

IX. Méthodologie

- Cours théoriques (Cybersécurité) avec participation des apprenants
- QCM
- Supports de formation
- Cas concrets, exemples pratiques

X. Évaluation de la formation

- QCM au début et à la fin de la formation
- Évaluation de satisfaction via un questionnaire
- Remise d'une attestation de formation

XI. Intervenant

- Nicolas Thore

XII. Contenu

Module 1 : La Cybersécurité (9h - 9h45)

Comprendre les enjeux de la cybersécurité pour une entreprise et identifier les formes courantes de cyberattaques.

- QCM
- Qu'est-ce que la cybersécurité
- Les cyberattaques
- Ce qu'il faut savoir
- Quelques chiffres cyber
- Exemple cyberattaque
- Une nouvelle économie

Module 2 : Les Systèmes d'Informations (9h45 - 10h15)

Savoir définir un système d'information et expliquer pourquoi il est un actif stratégique à protéger.

- Définition des Systèmes d'Informations
- Sécurité des Systèmes d'Informations
- Enjeux des Systèmes d'Informations
- Pourquoi les Systèmes d'Informations

Module 3 : Notions de vulnérabilité, menace, attaque (10h15 - 11h)

Différencier les notions de vulnérabilité, de menace et d'attaque afin de mieux appréhender les risques numériques.

- Vulnérabilité
- Menace
- Attaque

Module 4 : Différents types d'attaque (11h - 12h30)

Identifier les principales formes d'attaques et adopter les premiers réflexes en cas d'incident.

- Phishing
- Exemple
- Que faire
- Rançongiciel
- Comment ça fonctionne
- Attaque DDOS
- Arnaque au président
- Sécurité Physique
- Ingénierie Sociale
- L'humain

Module 5 : Les bons réflexes (14h - 14h30)

Mettre en œuvre les bonnes pratiques numériques pour réduire les risques quotidiens.

- Mot de passe
- Sauvegardes
- Pièges quotidien (wifi public, clé usb, mises à jour …)
- Pro / Perso
- Réseaux Sociaux
- Cloud
- Télétravail et mobilité

Module 6 : Gestion de crise (14h30 - 15h)

Comprendre les étapes d'une gestion de crise cyber et adopter les bons réflexes face à une cyberattaque.

- PCA
- PRA
- Comment réagir en cas de cyberattaque

- Premiers gestes
- Piloter la crise
- Gérer la crise
- Sortir de crise

Module 7 : Obligations Légales & conformité (15h - 15h30)

Identifier les obligations légales en matière de cybersécurité et les implications concrètes pour l'entreprise.

- RGPD c'est quoi ?
- Notions clés web
- Traitement des données
- Conseils
- CNIL
- NIS2

Module 8 : Darkweb (15h30 - 16h)

Découvrir le fonctionnement du darkweb et évaluer les risques liés à l'exposition des données de l'entreprise.

- Le Darkweb c'est quoi ?
- Surface web
- Deepweb et Darkweb

Module 9 : Etude de Cas et jeu (16h- 17h)

Appliquer les connaissances acquises à travers une mise en situation pratique pour renforcer la mémorisation des réflexes à adopter.