

Sensibilisation 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

- 1/2 jour (4h)

IV. Lieu et horaire

- En intra
- Les cours ont lieu de 9h à 13h

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 : 01.89.27.24.06 / contact@guiddy.fr

VIII. Objectifs de la formation

- Comprendre les enjeux essentiels de la cybersécurité
- Reconnaître les principales menaces
- Appliquer les bonnes pratiques au quotidien
- Savoir réagir face à un incident

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
- Pourquoi la cybersécurité nous concerne tous
- Quelques chiffres cyber
- Exemple cyberattaque
- Une nouvelle économie

Module 2 : Les Principales Menaces (9h45 - 10h30)

Identifier les principales formes d'attaques

- Phishing
- Rançongiciel
- Attaque DDOS
- Arnaque au président
- Ingénierie Sociale
- L'humain

Module 3 : Les bons réflexes (10h30 - 11h15)

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 4 : Gestion de crise (11h15 - 11h45)

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

Module 5 : Obligations Légales & conformité (11h45 - 12h15)

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

- RGPD
- CNIL
- NIS2

Module 6 : Cas pratique et Echange (12h15- 13h)

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