SYS-CONNECT
L'INFORMATIQUE A L'ÉCOUTE DE VOS BESOINS

FORMATION
SENSIBILISATION A LA CYBER-SECURITE
Durée : 1 Journée (7H)
Tarif sur demande

Objectifs généraux

- ∇ **Comprendre les enjeux de la cyber-sécurité**
- ∇ **Adopter les bonnes pratiques au quotidien**
- ∇ **Identifier les risques (phishing, malwares, ingénierie sociale, …)**
- ∇ **Réagir efficacement en cas d'incident**

Prérequis

- ✓ **Formation en français**
- ✓ **Accessible à tous les niveaux**
- ✓ **Formation en distanciel (FOAD)**
- ✓ **Nécessite une connexion internet ainsi que d'un ordinateur ou d'une tablette pour suivre la formation**
- ✓ **Attestation de fin de formation**

1. Evaluation du niveau initial

Durée : 30 min
Objectif : Se positionner, personnaliser la formation

- **QCM :** Niveau de connaissance et de conscience en cybersécurité (vocabulaire, réactions aux différents scénarios)
- **Résultats :** Score & Profil de risque par catégories (mots de passe, vigilance emails, navigation, usage pro/perso, ect.)

2. Fondamentaux de la Cyber-Sécurité

Durée : 1H00
Objectif : Comprendre les notions de bases et identifier les rôles

- **Définitions clés :** malware, ransomware, phishing, RSSI, ect.
- **Exemples concrets d'attaques :** cas réels et analyse d'attaque fictive
- **Impacts :** financiers, juridiques, réputations

3. Menaces & Risques Concrets

Durée : 1H30
Objectif : Identifier de détecter les différents types de menaces

- **Comprendre les différentes menaces :** phishing, ingénierie sociale, ect.
- **Identifier et expliquer les différentes menaces :** Simulations, quizz, analyse de mails et de pages web suspectes

4. Les bonnes pratiques utilisateur

Durée : 1H30

Objectif : Appliquer les règles de sécurité au quotidien

- **Comprendre les bonnes pratiques :** politique de mots de passe, navigation web, WIFI, périphériques USB, ect.
- **Mettre en œuvre les bonnes pratiques :** Mots de passe, utilisations de l'outil informatique, check-list des bonnes pratiques.

5. Réagir en cas d'incident

Durée : 1H30

Objectif : Adopter les bons réflexes et connaitre les procédures internes

- **Adopter les bons réflexes :** Quoi faire (et ne pas faire), qui prévenir.
- **Connaitre & utiliser les procédures internes :** Lecture des procédures internes et élaboration d'un plan de réaction personnel

6. Evaluation finale

Durée : 1H

Objectif : Valider la montée en compétence et l'appropriation des réflexes de sécurité

- **QCM final :** Fondamentaux de la cyber-sécurité
- **Mise en situation :** mail suspect, bonne pratiques, réflexes à avoir