# PROGRAMME DÉTAILLÉ

## CYBERSÉCURITÉ SENSIBILISATION

### MODALITÉS ET DURÉES :

**Durée** : 7h – 100 % distanciel

**Répartition** :

- **Synchrone** : 2 classes virtuelles de 3h (6h)
- **Asynchrone** : 1h

### PUBLIC VISÉ :

Salariés de TPE/PME souhaitant acquérir les bons réflexes face aux risques numériques, quel que soit leur service ou niveau technique.

### PREREQUIS

Matériel informatique, casque micro et connexion internet dans le cadre des formations en distanciel.
Un test de positionnement est à réaliser en amont de la formation et conditionne l'accès à la formation adapté au niveau et objectifs de l'apprenant.

### OBJECTIFS PÉDAGOGIQUE :

- Comprendre les menaces actuelles en cybersécurité, adopter des comportements numériques responsables, identifier les données critiques de l'entreprise, réagir efficacement en cas d'incident et contribuer à la mise en œuvre d'une charte informatique interne.

### CONTENU PÉDAGOGIQUE :

**Session 1 : Comprendre les risques et sécuriser ses usages (3h)**

- Introduction à la cybersécurité : définitions, panorama des risques actuels (0,5h)
- Identifier les menaces courantes : phishing, malwares, ransomwares, faux sites, ingénierie sociale (0,75h)
- Reconnaitre les signaux d'alerte : liens suspects, pièces jointes, fautes d'orthographe, comportements inhabituels (0,5h)
- Bonnes pratiques au quotidien : gestion des mots de passe, navigation sécurisée, vigilance sur smartphone (0,5h)
- Atelier : étude collective de scénarios réels de cyberattaque – analyse d'un faux mail, simulation de vol de données (0,75h)

**Temps asynchrone (1h) :**

- Vidéo : Les 10 erreurs humaines les plus fréquentes en cybersécurité (0,2h)
- Micro-module : Bonnes pratiques pour sécuriser ses mots de passe (0,2h)
- Étude de cas interactif : Réagir face à une tentative de phishing (0,3)
- Capsule vidéo : Sécuriser son poste de travail, ses connexions et ses outils cloud (0,1)
- Lecture guidée : Charte informatique – les indispensables à intégrer (0,2h)

**Session 2 : Développer les compétences essentielles en management opérationnel (3h)**

- Quelles données sont à protéger ? Données personnelles, professionnelles, stratégiques (0,5h)
- Sauvegardes, mises à jour, antivirus, VPN : construire un socle de sécurité (0,5h)
- Travailler à distance en toute sécurité : Wifi public, BYOD, messageries, outils collaboratifs (0,5h)
- Responsabilités de l'utilisateur : confidentialité, RGPD, traçabilité (0,5h)
- Construire et diffuser une charte informatique : rédaction des bonnes pratiques adaptées à son métier (0,5h)
- Atelier final : formalisation des 7 réflexes cybersécurité à intégrer dans l'organisation (0,5h)

## RESSOURCES MOBILISÉES :

- Présentations animées, quiz, cas pratiques, fiches téléchargeables
- Plateforme e-learning avec accès 24/7
- Capsules vidéo pédagogiques et infographies interactives
- Suivi intégré (quiz auto-évalués, ancrage par cas pratiques)