Sensibilisation à la Cybersécurité

Objectifs pédagogiques :

A l'issue de la formation, les participants seront capables de comprendre les principaux risques liés à l'utilisation des outils numériques, identifier les menaces cyber les plus courantes dans leur environnement professionnel, adopter les bons réflexes pour protéger les informations et les données sensibles, réagir de manière appropriée face à une situation suspecte ou un incident de sécurité, contribuer activement à la sécurité du système d'information de l'entreprise

Durée :	Prérequis :	Public concerné :	Tarif HT/jour*
1 jour (7 h)	Aucun	Tous publics.	Nous consulter

Contenu de la formation

Introduction

- Accueil, présentation du formateur, de la démarche, des modalités de réalisation
- Présentation des participants et de leurs attentes
- Rappel des objectifs définis, validation par les participants
- Approche de l'outil et de méthodes de travail liées à son utilisation

Comprendre les enjeux de la Cybersécurité

- Pourquoi la cybersécurité concerne tous les collaborateurs
- Les idées reçues et les comportements à risque
- Les actifs essentiels à protéger (données, image, continuité d'activité)
- Panorama des menaces numériques actuelles

Rôles et responsabilités en matière de sécurité

- Responsabilité individuelle et collective
- Rôle de la direction et des managers
- Missions de la DSI, du RSSI et des équipes techniques
- Protection des données personnelles et rôle du DPO
- Place des prestataires et partenaires externes
- Attentes vis-à-vis des utilisateurs

Cadre de référence et règles internes

- Politiques de sécurité et chartes informatiques
- Bonnes pratiques, guides utilisateurs et procédures internes
- Pourquoi ces règles existent et comment les appliquer au quotidien

Sensibilisation à la Cybersécurité

Objectifs pédagogiques :

A l'issue de la formation, les participants seront capables de comprendre les principaux risques liés à l'utilisation des outils numériques, identifier les menaces cyber les plus courantes dans leur environnement professionnel, adopter les bons réflexes pour protéger les informations et les données sensibles, réagir de manière appropriée face à une situation suspecte ou un incident de sécurité, contribuer activement à la sécurité du système d'information de l'entreprise

Durée :	Prérequis :	Public concerné :	Tarif HT/jour*
1 jour (7 h)	Aucun	Tous publics.	Nous consulter

Notions clés du cadre légal et réglementaire

- Responsabilités liées à l'utilisation des outils numériques
- Obligations professionnelles et contractuelles
- Protection des données personnelles et respect de la vie privée
- Usage professionnel et personnel des ressources informatiques

Menaces et techniques d'attaque

- Divulgation involontaire d'informations
- Ingénierie sociale et manipulation des utilisateurs
- Espionnage économique et fuite d'informations
- Exploitation des comportements humains

Principaux risques cyber rencontrés par les utilisateurs

- Vol ou perte d'informations
- Logiciels malveillants et infections
- Phishing et tentatives d'escroquerie
- Usurpation d'identité numérique
- Risques liés aux réseaux sociaux et aux usages collaboratifs

Evaluer la sensibilité de l'information

- Identifier les informations sensibles
- Comprendre les impacts potentiels (juridiques, financiers, image, activité)
- Hiérarchiser les niveaux de sensibilité
- Éviter les erreurs courantes d'évaluation

Sensibilisation à la Cybersécurité

Objectifs pédagogiques :

A l'issue de la formation, les participants seront capables de comprendre les principaux risques liés à l'utilisation des outils numériques, identifier les menaces cyber les plus courantes dans leur environnement professionnel, adopter les bons réflexes pour protéger les informations et les données sensibles, réagir de manière appropriée face à une situation suspecte ou un incident de sécurité, contribuer activement à la sécurité du système d'information de l'entreprise

Durée :	Prérequis :	Public concerné :	Tarif HT/jour*
1 jour (7 h)	Aucun	Tous publics.	Nous consulter

Adopter les bons comportements au quotidien

- Bonnes pratiques sur le lieu de travail
- Vigilance en déplacement et en télétravail
- Protection des informations en dehors de l'entreprise

Gestion sécurisée des supports et des données

- Utilisation sécurisée des documents papier
- Stockage et partage dans des environnements collaboratifs
- Sécurité des postes fixes et des équipements mobiles
- Cycle de vie de l'information : création, stockage, transmission, suppression

Utilisation sécurisée des outils numériques

- Sécurisation des postes de travail et des appareils mobiles
- Gestion des mots de passe et authentification
- Bonnes pratiques de communication (email, web, cloud)
- Télétravail, accès distants et VPN
- Sauvegarde, archivage et destruction des données

Conclusion et engagement des utilisateurs

- Synthèse des messages clés
- Responsabilités individuelles
- Engagement personnel en faveur de la cybersécurité

Clôture de la formation

- Récapitulatif
- Conseils, trucs et astuces
- Fiche d'évaluation, synthèse
- Récupération par les participants des fichiers travaillés et des exemples traités

Sensibilisation à la Cybersécurité

Objectifs pédagogiques :

A l'issue de la formation, les participants seront capables de comprendre les principaux risques liés à l'utilisation des outils numériques, identifier les menaces cyber les plus courantes dans leur environnement professionnel, adopter les bons réflexes pour protéger les informations et les données sensibles, réagir de manière appropriée face à une situation suspecte ou un incident de sécurité, contribuer activement à la sécurité du système d'information de l'entreprise

Durée :	Prérequis :	Public concerné :	Tarif HT/jour*
1 jour (7 h)	Aucun	Tous publics.	Nous consulter

Les méthodes et critères d'évaluation pédagogique

La constitution des groupes homogènes s'établira à partir d'un outil d'évaluation. L'évaluation permettra d'avoir un premier aperçu du niveau de l'apprenant, de ses connaissances et de ses attentes pour la formation appropriée.
Une approche pédagogique sera réalisée par le formateur avant le début de la formation, afin d'adapter le contenu du programme pour répondre aux attentes des apprenants.
Une attestation est fournie à l'apprenant à l'issue de la formation validant les connaissances acquises lors de la formation.

Les méthodes pédagogiques

Chaque thème du programme sera accompagné d'ateliers pratiques avec suivi et assistance personnalisée.
Les ateliers pourront être réadaptés en fonction des propres modèles des participants.

Le suivi et les moyens pédagogiques

Un support de formation sera transmis à chacun des participants, reprenant les principaux thèmes de la formation réalisé sous forme de captures d'écran et d'explications de texte.
Les apprenants repartent à l'issue de la formation avec les fichiers travaillés pendant la formation ainsi que les coordonnées du formateur, ce qui leur permettra d'échanger avec ce dernier et de lui poser toute question relative à la formation suivie sans limitation de durée.
Une feuille d'émargement est signée par les stagiaires (matin et après-midi) chaque jour de la formation, afin d'attester de leur présence.

Les moyens techniques

Salle équipée avec un poste par personne, un tableau blanc, un paperboard, un accès wifi et un vidéo projecteur.