+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 27/03/2025

S'inscrire

Formation sécuriser ses pratiques numériques

1 jour (7 heures)

Présentation

Notre formation sécuriser ses pratiques numériques vous apprendra tout ce qu'il faut savoir sur les enjeux liés aux bonnes pratiques de CyberSécurité dans les entreprises ainsi que les différentes réglementations encadrant les données personnelles.

De nos jours, les lois encadrant la protection des données personnelles se multiplient. Que ce soit pour protéger les entreprises des cybermenaces ou pour protéger les droits des consommateurs, il est crucial de connaitre les enjeux et les réglementations qui régissent le marché.

Notre programme de formation vous apprendra non seulement des connaissances théoriques sur la cybervigilance et l'encadrement des données personnelles, mais également des compétences pratiques dans l'utilisation d'outils pour protéger votre matériel informatique et dans l'acquisition de bonnes pratiques à adopter au quotidien.

Objectifs

- Comprendre les enjeux de la CyberSécurité en entreprise
- Se sensibiliser au cadre réglementaire (RGPD)
- Identifier les principaux risques informatiques (hameçonnage, rançongiciels, failles humaines, etc.)
- Mettre en place les bonnes pratiques de sécurité
- Utiliser des outils simples et efficaces pour sécuriser les équipements et les échanges numériques
- Prévenir et gérer les risques liés aux attaques numériques (identifier les acteurs et les bons réflexes à avoir en cas d'attaque)
- Diffuser et développer des réflexes sécuritaires adaptés dans son activité quotidienne

Public visé

- Toute personne travaillant en milieu professionnel
- Toute personne ayant une infrastructure à protéger
- Toute personne manipulant des données personnelles

Pré-requis

- Connaissances générales en informatique

Programme de notre formation sécuriser ses pratiques numériques (Cybersécurité / RGPD)

Enjeux de la Cybersécurité dans les entreprises

- Pourquoi la Cybersécurité est un enjeu majeur pour les entreprises de toutes tailles ? (augmentation des cyberattaques et impact sur l'activité)
- Cybercriminalité : une menace internationale décuplée avec l'IA
- Conséquences possibles d'un manque de vigilance en sécurité (pertes financières, arrêt de production, sanctions légales, image négative)
- Lexique utile (CNIL, ANSSI, RSSI, DPO, BYOD, Blue / Red Team, logs, etc.)
- Le rôle de chaque employé dans la Cybersécurité : les comportements individuels peuvent protéger ou mettre en danger l'entreprise
- Les statistiques marquantes
- Retour sur les incidents médiatisés (retail, santé, télécom...)
- Atelier pratique : Étude de cas sur une cyberattaque réelle, analyse par les participants des erreurs commises et discussion des solutions pour les éviter à l'avenir

Le cadre réglementaire (RGPD)

- Principes fondamentaux du RGPD (Règlement général sur la protection des données)
- Objectif de protection des données personnelles
- Obligations légales pour les entreprises et droits des utilisateurs (accès, rectification, effacement de leurs données)
- Bonnes pratiques pour la conformité RGPD au quotidien
- Risques en cas de non-conformité
- Ouverture et présentation rapide de NIS2, DORA, et Cyber Resilience Act (CRA)
- Atelier pratique : Mise en situation d'une entreprise fictive où certaines pratiques ne respectent pas le RGPD. Identifier les non-conformités et proposer des mesures correctives.

Bonnes pratiques de sécurité au quotidien

- Adopter une politique de mots de passe solides
- Sécuriser ses équipements de travail (PC, smartphone) avec des outils
- Bonnes pratiques face aux e-mails et pièces jointes
- Protéger les données sensibles de l'entreprise
- Bonnes pratiques lors du télétravail ou en déplacement
- Atelier pratique : Entraînement aux bonnes pratiques.

Utilisation d'outils de cybersécurité simples

- Outils de base pour se protéger
  - antivirus
  - pare-feu personnel
  - mises à jour automatiques (OS, Firmware, Drivers)
  - Politique de chiffrement et sauvegarde
- Utiliser un gestionnaire de mots de passe
- Authentification à deux facteurs (2FA)
- Naviguer sur le web de façon sécurisée (VPN)
- Échanger de manière sécurisée (ex: Signal)
- Faire sa veille "Cyber Threat Intelligence"
- Atelier pratique : Construire sa checklist de bonnes pratiques
- Ouverture vers des techniques plus avancées (IAM, Zero Trust, CDN, etc.)

Prévention des risques liés et cybermenaces

- Tour d'horizon cybermalveillance.gouv.fr (le portail gouvernemental français) & l'ANSSI
- Identifier les principales cybermenaces actuelles :
  - hameçonnage (phishing)
  - rançongiciel (ransomware)
  - malware (virus, logiciels espions)
  - attaques par ingénierie sociale.
- Comprendre les méthodes employées par les attaquants
- Appliquer des mesures préventives au quotidien
- Savoir réagir face à un doute
- Alerter le CERT-FR
- Atelier pratique : Simulation de menace, analyse collective d'un email de phishing fictif reçu par un employé, afin d'identifier les indices d'arnaque et de décider des actions à entreprendre (suppression, signalement).

Développement des bons réflexes sécuritaires

- Intégrer la sécurité dans sa routine de travail
- Renforcer la culture sécurité en entreprise et formation de ses équipes
- Présentation du MOOC de l'ANSSI
- Maintenir sur le long terme les bonnes habitudes acquises
- Atelier pratique : Conclusion interactive, quiz final couvrant les points clés de la formation, suivi d'un échange où chaque participant décrit un réflexe sécuritaire qu'il s'engage à appliquer au quotidien.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant

d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.