Mis à jour le 22/08/2025

S'inscrire

Formation cybersécurité pour tous : bonnes pratiques et hygiène numérique

1 jour (7 heures)

Présentation

Notre formation « La cybersécurité pour tous : bonnes pratiques et hygiène numérique » s'adresse à l'ensemble des collaborateurs souhaitant comprendre les risques numériques et adopter les bons réflexes au quotidien pour sécuriser leurs usages professionnels.

Vous découvrirez comment intégrer les bonnes pratiques de sécurité numérique dans votre activité, depuis la gestion des mots de passe et la protection des terminaux jusqu'à la détection des menaces courantes et la réaction en cas d'incident. Nous aborderons également l'impact des nouvelles technologies, notamment l'intelligence artificielle, qui bouleversent à la fois les méthodes d'attaque (phishing plus crédible, usurpation d'identité, deepfakes) et les solutions de défense.

Au fil de cette journée, vous apprendrez à reconnaître les menaces les plus courantes, telles que le phishing, les ransomwares ou encore l'usurpation d'identité, qui touchent aujourd'hui tous les environnements professionnels. Vous verrez également quels sont les bons réflexes à adopter pour protéger vos outils numériques au quotidien, depuis la gestion sécurisée des mots de passe jusqu'aux mises à jour, sauvegardes régulières et bonnes pratiques sur l'ensemble de vos équipements numériques (PC, portables, smartphones, tablettes).

La formation vous guidera aussi sur la conduite à tenir en cas de suspicion d'incident afin de réagir efficacement sans aggraver la situation. Enfin, vous découvrirez comment chacun peut contribuer à développer une véritable culture de cybersécurité au sein de son organisation, en partageant les bonnes pratiques et en renforçant la vigilance collective.

À l'issue de la formation, vous serez capable d'identifier les principaux risques, de renforcer votre vigilance face aux cyberattaques et de sécuriser vos usages numériques au quotidien, tout en contribuant à diffuser les bonnes pratiques au sein de votre équipe et de votre organisation.

Objectifs

- Comprendre les enjeux de la cybersécurité dans un contexte professionnel.
- Identifier les principales menaces informatiques et les comportements à risque.
- Adopter les bonnes pratiques pour garantir une hygiène numérique efficace au quotidien.

Public visé

- Toutes personnes souhaitant connaître les bonnes pratiques de la cybersécurité.

Pré-requis

- Aucun prérequis

Programme de notre Formation cybersécurité pour tous : bonnes pratiques et hygiène numérique

[Jour 1 - Matin]

Introduction : pourquoi la cybersécurité concerne tout le monde ?

- Panorama des enjeux : coûts d'une faille, impacts réputationnels, continuité d'activité
- Exemples concrets : attaques récentes dans les PME, hôpitaux, collectivités
- Les risques dans le quotidien de chacun (messaging, navigation web, réseaux sociaux, usages mobiles)
- Notions simples de gouvernance et de responsabilité (qui fait quoi en entreprise ?)
- Atelier pratique : Décryptage d'une actualité cyber et identification des erreurs humaines en cause.

Menaces courantes et comportements à risque

- Reconnaître les attaques les plus fréquentes : phishing, ransomware, usurpation d'identité, faux support technique
- Les erreurs humaines les plus courantes (clic intempestif, mot de passe faible, usage perso/pro confondu)
- L'évolution des menaces avec l'IA : phishing "intelligent", deepfakes et usurpations plus crédibles
- Bonnes pratiques pour réduire les risques (hygiène numérique accessible à tous)
- Atelier pratique : Analyse de mails suspects (avec de vrais exemples), tri entre mails légitimes et phishing.

[Jour 1 - Après-midi]

Adopter une bonne hygiène numérique

- Les bons réflexes au quotidien
- Gestion des mots de passe (MFA, coffre-fort de mots de passe)
- Sauvegardes et mises à jour régulières
- Sécurisation des terminaux (PC, smartphones, tablettes)
- Gestion des accès et verrouillage des postes
- Bonnes pratiques de mobilité (Wi-Fi public, télétravail)
- Atelier pratique : Mise en place de ses "10 règles personnelles de cybersécurité".

Réagir efficacement face à un incident

- Reconnaître les signaux d'alerte
- Que faire (et ne pas faire) en cas de suspicion d'attaque ?
- Procédures d'alerte et d'escalade dans un environnement professionnel
- Mise en situation : Simulation d'une attaque par phishing. Réaction individuelle et collective, débrief.

Créer une culture cyber au travail

- Partager les bonnes pratiques avec ses collègues
- Intégrer la cybersécurité dans ses habitudes quotidiennes
- Approche collective : ambassadeurs cyber, rappels réguliers
- Anticiper les évolutions : rester vigilant face aux nouveaux usages numériques et à l'exploitation croissante de l'IA par les attaquants
- S'informer régulièrement grâce à une veille adaptée : Consulter des alertes simples (ANSSI, CNIL, CERT-FR simplifiées), suivre les communications internes de l'entreprise, utiliser des supports de sensibilisation (affiches, newsletters, capsules vidéo courtes).

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.