ACE MULTIPASS
Cybersécurité - Méthodes agiles

FICHE DE FORMATION

Organisme de formation

Formation Sensibilisation À La Cybersécurité

Formation de 4 heures pour acquérir les fondamentaux de la cybersécurité et adopter les bons réflexes au quotidien, en contexte professionnel comme personnel, à travers des ateliers pratiques et interactifs (Bitwarden, Have I Been Pwned, chiffrement…).

DURÉE	PRIX	HORAIRES
4 heures	**450 €**	**Créneau de 4h** *(matinée ou après-midi)*

PRÉSENTATION

Cette formation permet d'acquérir les fondamentaux de la cybersécurité et d'adopter les bons réflexes au quotidien, en contexte professionnel comme personnel. Elle présente les principales situations à risque ainsi que les bonnes pratiques essentielles pour limiter les menaces.

Les participants travaillent sur la gestion des mots de passe et des comptes à travers un atelier Bitwarden. Les risques liés aux emails et à la navigation web sont abordés de manière concrète, notamment via un atelier Have I Been Pwned pour sensibiliser à l'exposition des données.

La protection de l'environnement de travail est également traitée, avec les bonnes pratiques liées à la sécurité des postes, aux sauvegardes et au chiffrement des données, illustrés par un atelier.

La formation couvre enfin la signature électronique, les usages nomades, la distinction entre usages professionnels et personnels, ainsi que les enjeux de sécurité physique.

Une approche pratique et interactive permet une mise en application immédiate des bonnes pratiques de cybersécurité.

Note : cette formation peut aussi être organisée en intra dans les locaux de votre entreprise.

OBJECTIFS PÉDAGOGIQUES

À l'issue de cette formation, l'apprenant sera capable de :

- Définir et appliquer les bonnes pratiques de cybersécurité au quotidien.
- Identifier les principaux risques liés aux données personnelles et professionnelles.
- Comprendre les impacts des usages numériques sur les environnements personnels et professionnels.
- Sécuriser ses accès et ses mots de passe à l'aide d'un gestionnaire dédié.
- Détecter une exposition ou une compromission de ses données.
- Adopter des réflexes de sécurité face aux emails, au web et aux usages nomades.

- Mettre en œuvre des mesures simples de protection des données (sauvegarde, chiffrement).

PUBLIC CIBLE ET PRÉREQUIS

Population visée : Ouvrier – Employé – Employé qualifié – Cadre – Cadre supérieur.

Public concerné : toute personne souhaitant se sensibiliser à la cybersécurité.

Pré-requis : aucun.

PROGRAMME

Module 1 · Introduction & concepts

- Les enjeux
- Le RGPD
- Les concepts en cybersécurité
- Vulnérabilités, menaces, attaques

Module 2 · Les situations à risque

- Le délicat équilibre entre productivité et sécurité
- Hameçonnage & ingénierie sociale
- Déroulement d'une attaque avancée
- Fraude interne
- Sécurité du personnel
- Violations d'accès non autorisé
- Virus
- Déni de service (DDoS)
- Le BYOD (Bring Your Own Device)

Module 3 · Les bonnes pratiques

- Mots de passe, comptes
- Email et web
- Authentification forte, clés YubiKey

Atelier — Gestionnaire de mots de passe.

Démo — Activation de l'authentification à deux facteurs.

Atelier — Have I Been Pwned.

Module 4 · Protection de l'ordinateur

- Applications
- Mises à jour
- Antivirus
- Mot de passe BIOS
- Durcissement

Module 5 · Sauvegarde, chiffrement

- Chiffrement de disque
- Sauvegardes
- Supports de sauvegarde

Atelier — 7-Zip.

Démo — Microsoft BitLocker.

Module 6 · Signature électronique

- Les bases de la cryptographie
- Les algorithmes symétriques et asymétriques
- Les fonctions de hachage
- Les certificats
- Les jetons cryptographiques
- La signature électronique

Démo — Signature électronique de PDF avec une carte à puce.

Module 7 · Usages nomades

- Wifi publics
- Bornes de recharge
- VPN
- Précautions en déplacement

Module 8 · Usage pro vs perso

Module 9 · La sécurité physique

- Photocopieuses, imprimantes
- Sécurité des équipements (filtres écrans, antivols…)

Clôture — Quiz interactif de validation des acquis.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Chaque session peut être adaptée aux besoins des personnes en situation de handicap. Nous invitons les participants concernés à nous en informer avant le début de la formation, afin d'examiner ensemble les aménagements possibles : conditions d'accès aux salles, adaptation des supports et des méthodes pédagogiques, ou réorganisation du planning de la session.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

L'animation des sessions s'appuie sur des outils variés : supports audiovisuels, documents remis aux stagiaires, mises en application pratiques accompagnées de leurs corrigés pour les formations à vocation opérationnelle, et études de cas concrets ou retours d'expérience pour les sessions à caractère plus théorique.

À la fin de chaque session, ACE-MULTIPASS remet aux stagiaires un questionnaire de satisfaction, dont les résultats sont ensuite examinés par l'équipe pédagogique.

Une feuille de présence est signée à chaque demi-journée et remise en fin de parcours ; une attestation de suivi de formation est également délivrée aux stagiaires ayant participé à l'intégralité de la session.

COMPÉTENCES DU FORMATEUR

Nos intervenants sont choisis pour leur expertise dans les domaines qu'ils enseignent. Chacun est sélectionné par notre équipe pédagogique, qui vérifie à la fois sa maîtrise technique du sujet et ses aptitudes à transmettre et animer un groupe. Ils justifient généralement de cinq à dix ans d'expérience professionnelle au minimum, et occupent ou ont occupé des fonctions à responsabilité dans leur secteur d'activité.

MODALITÉS D'ÉVALUATION

Tout au long du parcours, le formateur mesure la progression des stagiaires à travers différents exercices : questionnaires à choix multiples, mises en situation ou exercices pratiques.

Un test de positionnement est par ailleurs réalisé avant et après la formation, afin de mesurer les compétences acquises par chaque participant.