DAWAN

Plan de la formation

www.dawan.fr

Formation Sécuriser ses pratiques numériques (cybersécurité / RGPD)

Durée :	1 jours (7 heures)
Tarif inter-entreprises :	775,00 CHF HT (Présentiel) 620,00 CHF HT (Distanciel)
Public :	Utilisateurs de PC sous Windows
Pré-requis :	Connaissances fondamentales de la bureautique, de la messagerie et d'interner
Objectifs :	Comprendre les enjeux de la cybersécurité en entreprise - Identifier les principaux risques liés à l'usage quotidien des outils numériques - Appliquer les bonnes pratiques pour sécuriser leurs équipements et données - Réagir efficacement en cas de tentative d'attaque ou de fuite de données
Modalités pédagogiques, techniques et d'encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l'Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat. • Un formateur expert.
Modalité d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	CYB102475-F
Note de satisfaction des participants :	Pas de données disponibles

Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d'accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Comprendre les enjeux de la cybersécurité dans les entreprises

Pourquoi la cybersécurité est un enjeu majeur ?
Exemples d’attaques impactant les entreprises
Conséquences d’un manque de vigilance (pertes financières, atteinte à la réputation, sanctions légales)

Atelier pratique : étude de cas sur des cyberattaques ayant touché des entreprises de différents secteurs. Les participants analyseront les erreurs commises et proposeront des solutions pour les éviter.

Sensibilisation au cadre réglementaire (RGPD)

Les principes fondamentaux du RGPD
Obligations des entreprises et droits des utilisateurs
Bonnes pratiques pour la protection des données personnelles

Atelier pratique : mise en situation où les participants devront identifier des pratiques non conformes au RGPD dans des scénarios de travail courants et proposer des solutions pour y remédier.

Identifier les principaux risques informatiques

Hameçonnage (phishing) : comment le reconnaître ?
Rançongiciels : fonctionnement et impact
Failles humaines : mots de passe faibles, négligence, ingénierie sociale
Autres menaces courantes : malwares, faux sites web, usurpation d’identité

Atelier pratique : simulation d’une tentative de phishing où les participants analyseront des emails suspects pour identifier les indices révélateurs d’une attaque.

Mettre en place les bonnes pratiques de sécurité

Création et gestion de mots de passe sécurisés
Sécurisation des équipements (PC, smartphone, accès Wi-Fi)
Détection et gestion des emails suspects
Protection des données sensibles (chiffrement, sauvegardes)
Gestion des accès et bonnes pratiques pour le travail nomade

Atelier pratique : création et test de mots de passe sécurisés, configuration d'authentification à deux facteurs et exercices pratiques sur la reconnaissance des comportements à risque.

Utiliser des outils simples et efficaces pour sécuriser les équipements et les échanges numériques

Gestionnaires de mots de passe
Antivirus et pare-feu : comment bien les utiliser ?
Navigation sécurisée : VPN, extensions anti-tracking
Messageries sécurisées et bonnes pratiques pour les emails professionnels

Atelier pratique : installation et paramétrage d'un gestionnaire de mots de passe, test de navigation sécurisée avec un VPN et configuration des paramètres de sécurité d'un navigateur web.

Prévenir et gérer les risques liés aux attaques numériques

Que faire en cas de suspicion de cyberattaque ?
Signaler un incident : qui contacter et comment réagir ?
Exercices pratiques : simulation de phishing et analyse de cas concrets

Atelier pratique : mise en situation où les participants devront réagir face à un scénario d'attaque simulée et identifier les actions prioritaires à mettre en place.

Développer des réflexes sécuritaires adaptés dans son activité quotidienne

Adopter une posture de vigilance et sensibiliser ses collègues
Mises à jour régulières et bonnes habitudes à prendre
Test de validation des acquis (quiz et discussion interactive)

Atelier pratique : quiz final et échange collectif sur les bonnes pratiques à adopter en fonction des situations rencontrées par les participants.