DAWAN

Plan de la formation

www.dawan.fr

Formation Sensibilisation à la cybersécurité

Durée :	1 jours (7 heures)
Tarifs inter-entreprise :	875,00 CHF HT (standard) 700,00 CHF HT (remisé)
Public :	Tous les salariés de l'entreprise, quels que soient le service ou la fonction.
Pré-requis :	Utilisation courante des outils numériques (messagerie, web, bureautique)
Objectifs :	Découvrir les bonnes pratiques pour limiter les risques juridiques et opérationnels - Comprendre comment protéger les informations en adéquation avec les besoins métiers
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.
Modalités 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 :	CYB102741-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 son organisation

Découvrir ce que recouvrent les notions de sécurité informatique et de cybersécurité
Identifier les principaux types d'informations manipulées au quotidien (données clients, données RH, données stratégiques…)
Relier les incidents de cybersécurité à des risques concrets : juridiques, financiers, opérationnels, réputationnels
Prendre conscience du rôle de chaque salarié dans la protection de l'information
Atelier fil rouge : repérer, sur une journée type de travail, les informations sensibles que l'on manipule et les risques associés

Clarifier l'organisation et les responsabilités en matière de sécurité

Identifier les acteurs internes de la sécurité : direction, DSI, RSSI, DPO, managers, utilisateurs
Comprendre la répartition des responsabilités entre l'entreprise et chaque collaborateur
Repérer les règles et procédures internes qui encadrent l'usage des outils numériques
Savoir à qui s'adresser en cas de doute, de suspicion d'incident ou de perte de matériel
Atelier fil rouge : cartographier les interlocuteurs sécurité et les bons réflexes d'alerte dans son organisation

S'appuyer sur les référentiels SSI et vie privée

Découvrir les grandes familles de référentiels : sécurité des systèmes d'information (SSI) et protection des données personnelles
Comprendre en quoi ces référentiels se traduisent dans le quotidien (mots de passe, droits d'accès, confidentialité, RGPD…)
Identifier les principaux documents de référence internes : charte informatique,

politiques de sécurité, guides utilisateurs
Relier ces règles à la protection des personnes, des clients et de l'entreprise
Atelier fil rouge : retrouver et analyser un extrait de charte informatique ou de consignes internes de sécurité

Avoir une vision synthétique des obligations légales

Comprendre les grandes lignes des obligations en matière de protection des données personnelles et de sécurité
Identifier les risques en cas de non-respect : sanctions, responsabilité de l'entreprise, impact sur l'emploi et l'activité
Comprendre la notion de devoir de confidentialité et de respect du secret professionnel ou des informations sensibles
Relier la sécurité à la confiance des clients, des partenaires et des salariés
Atelier fil rouge : analyser de manière simple un exemple d'incident et ses conséquences juridiques et opérationnelles

Identifier les menaces et les risques au quotidien

Découvrir les menaces les plus fréquentes : phishing, ransomware, vol ou perte de matériel, erreurs d'envoi, divulgation involontaire
Différencier menace, vulnérabilité et risque à travers des exemples concrets
Comprendre que les risques ne sont pas uniquement techniques mais aussi organisationnels et humains
Prendre conscience des situations à risque dans son activité courante (déplacements, télétravail, travail en open-space…)
Atelier fil rouge : repérer des situations à risque dans des scénarios de vie quotidienne au bureau et en télétravail

Évaluer la sensibilité de l'information manipulée

Différencier information publique, interne, confidentielle, stratégique
Apprendre à se poser les bonnes questions : qui peut voir cette information, quelles seraient les conséquences en cas de fuite ?
Adapter son comportement en fonction de la sensibilité : modes de stockage, partage, conditions de consultation
Utiliser les règles internes de classification s'il en existe (marquage, niveaux de confidentialité)
Atelier fil rouge : classer différents types d'informations selon leur sensibilité et proposer des mesures de protection adaptées

Adopter les bonnes pratiques de comportement général

Appliquer les réflexes de base : verrouiller sa session, protéger ses mots de passe, se méfier des pièces jointes et liens suspects
Identifier les signaux d'alerte dans les mails et messages (phishing, fraude au président, faux support informatique…)
Respecter la discrétion dans les lieux publics et partagés (open-space, transports, salles de réunion, téléphone)
Savoir quoi faire immédiatement en cas de doute ou d'incident (alerte, isolement, ne pas cacher l'erreur)
Atelier fil rouge : analyser des exemples d'emails et de situations pour distinguer comportements sûrs et comportements risqués

Sécuriser l'utilisation des supports d'information sensible

Comprendre les risques liés aux clés USB, disques externes, impressions papier, carnets de notes, captures d'écran
Adopter de bonnes pratiques pour la conception, le stockage, le partage et la destruction des documents sensibles
Être vigilant lors des échanges : envoi de pièces jointes, outils de partage de fichiers, messageries instantanées
Appliquer des règles simples pour la fin de vie des supports (papiers, matériels, anciens fichiers, sauvegardes locales)
Atelier fil rouge : lister les supports utilisés dans son travail et définir les bonnes pratiques pour chacun

Utiliser de façon responsable les ressources du système d'information

Comprendre les règles d'usage des équipements (PC, smartphone, tablette, outils collaboratifs, cloud, Wi-Fi invité)
Distinguer usages professionnels et usages personnels acceptables ou non
Adopter de bonnes pratiques en mobilité : connexions sécurisées, Wi-Fi publics, documents affichés à l'écran
Contribuer à la sécurité globale en respectant mises à jour, consignes et consignes ponctuelles en cas d'incident majeur
Atelier fil rouge : construire une courte check-list personnelle « bons réflexes numériques » à appliquer chaque jour

Conclusion et engagement individuel

Synthétiser les principaux risques et les bonnes pratiques clés à retenir
Relier la cybersécurité à la qualité de service, à l'image de l'entreprise et à la

protection des personnes
Identifier les changements concrets que chacun peut mettre en œuvre dès la fin de la formation
Formaliser son engagement à adopter de meilleurs réflexes dans son activité quotidienne
Atelier fil rouge final : rédiger un engagement personnel de 3 à 5 actions simples à mettre en place dans le mois suivant