PROGRAMME DE FORMATION

Cybersécurité -1 Panorama SSI

Cybersécurité & Protection des données

RÉFÉRENCE	VERSION	ÉDITION	DOMAINE
WF-0262	V2026-005	2 novembre 2026	Cybersécurité & Protection des données

DURÉE	MODALITÉ	PROGRAMME	SANCTION
26 h	Distanciel asynchrone (e-learning) · Présentiel	11 modules 31 leçons	Attestation et certificat de réalisation

Objectifs pédagogiques

Expliquer les enjeux de la sécurité des systèmes d'information : actifs, besoins de disponibilité, d'intégrité et de confidentialité, conséquences d'un incident.

Reconnaître les principales menaces et techniques d'attaque, dont l'hameçonnage et la fraude par ingénierie sociale, et y réagir.

Conduire une analyse de risque simplifiée sur une activité de l'entreprise et proposer des mesures proportionnées.

Situer les obligations juridiques (protection des données, NIS 2 selon sa transposition, cybercriminalité) et les acteurs publics de la cybersécurité.

Appliquer et faire appliquer les règles d'hygiène : identités et accès, poste de travail, nomadisme, sauvegarde, prestataires et services en ligne.

Qualifier un incident, accomplir les premiers gestes, contribuer à la gestion de crise et aux déclarations.

Construire un plan d'action de sécurité et sensibiliser son équipe.

L'essentiel de la formation

Public visé

Dirigeants et managers de TPE et PME, référents informatiques non spécialistes, assistants, comptables, commerciaux et tout collaborateur qui veut comprendre les risques numériques de son entreprise et adopter les bons réflexes ; personnes en reconversion qui découvrent la sécurité des systèmes d'information.

Prérequis

Aucun prérequis de connaissances en informatique ou en sécurité. Comprendre et s'exprimer en français ; utiliser au quotidien un ordinateur, une messagerie et un navigateur.

Disposer d'un tableur et d'un traitement de texte pour remplir les modèles fournis. Connaître les outils de sa structure facilite les mises en situation ; un positionnement en début de parcours situe votre point de départ.

Modalités et déroulement

Formation à distance, accessible en ligne. Un positionnement ouvre le parcours. Chaque leçon part d'une courte mise en situation vidéo dans une PME industrielle fictive, avec des personnages animés récurrents (une directrice générale, un responsable informatique, une comptable, un commercial itinérant, une assistante, un prestataire d'infogérance), puis fait pratiquer : tri de messages piégés fictifs, scénarios à décisions, études de cas, repérage d'erreurs dans des politiques, des configurations décrites et des comptes rendus d'incident, échanges simulés et exercices sur les modèles fournis. Chaque module se termine par une mise en situation qui produit un livrable. Plus des deux tiers du temps de formation sont consacrés à la pratique. Personnes, entreprises et messages sont fictifs ; les règles, délais et recommandations ne sont jamais donnés de mémoire : chaque fiche méthode renvoie aux sources officielles relues à la date de production. Accompagnement par un formateur par messagerie.

Méthodes pédagogiques

- Positionnement en début de parcours
- Apports en vidéo : explications et démonstrations
- Mises en situation et scénarios à décisions
- Études de cas
- Exercices d'application et mises en pratique corrigées
- Production de livrables professionnels
- Quiz et QCM d'auto-évaluation
- Accompagnement et retours du formateur

Moyens pédagogiques et techniques

- Plateforme de formation en ligne, accès individuel à distance
- Vidéos pédagogiques
- Fiches méthode
- Modèles et supports téléchargeables
- Quiz et exercices interactifs en ligne
- Correction des productions sur grille de critères
- Messagerie avec le formateur

Modalités d'évaluation

Positionnement initial (non éliminatoire) ; retour détaillé sur chaque étude de cas, scénario et échange simulé ; correction des modèles déposés ; livrable de fin de module vérifié sur grille critériée ; quiz de module ; évaluation finale composée d'un cas complet (actifs et risques, hameçonnage, incident à qualifier et à gérer, plan d'action) et d'un questionnaire. Seuil de réussite interne : 70 % des critères du cas.

Sanction

Une attestation de fin de formation et un certificat de réalisation sont remis au participant sous réserve de la réalisation du parcours.

Cette formation n'est pas présentée comme préparant à une certification enregistrée : elle ne comprend ni inscription ni présentation à des épreuves de certification, et n'ouvre droit à aucune délivrance de certification ni au financement par le CPF.

Modalités et délais d'accès

La demande d'inscription peut être effectuée par téléphone, par courrier électronique ou au moyen du formulaire en ligne.

Un entretien ou un questionnaire de positionnement permet de vérifier l'adéquation de la formation avec les besoins, le niveau initial et les prérequis du candidat.

L'inscription devient définitive après validation du dossier administratif, acceptation des documents contractuels et, le cas échéant, confirmation du financement.

Les accès à la plateforme sont généralement activés sous 48 à 72 heures ouvrées après validation complète du dossier.

Les formations à distance sont proposées en entrées et sorties permanentes, sous réserve des délais ou dates imposés par le financeur ou le certificateur.

Accessibilité aux personnes en situation de handicap

Vidéos sous-titrées et transcrites, dialogues aussi disponibles en texte, messages piégés aussi décrits en texte, fiches méthode et modèles compatibles avec les lecteurs d'écran, navigation au clavier. Référent handicap joignable à handicap@will-formation.com pour étudier toute adaptation (durée, supports, outils).

Tarif de la formation

Prix : **1 710 €**

Financement : prise en charge possible par les organismes financeurs, selon les critères d'éligibilité applicables.

Qualiopi processus certifié

La certification qualité a été délivrée au titre de la catégorie d'action suivante : ACTIONS DE FORMATION. Certificat QUA25070009. WILL FORMATION — Société par actions simplifiée à associé unique au capital de 30 000 € — NDA 11757059675 (cet enregistrement ne vaut pas agrément de l'État) — SIRET 893 713 180 00014 — 01 85 09 25 99 — info@will-formation.com — www.will-formation.com

Programme détaillé

11 modules, 31 leçons — durée totale 26 h.

01 Positionnement

1. Positionnement — vos réflexes numériques

02 Les enjeux de la sécurité numérique

1. Ce que l'entreprise doit protéger
2. Disponibilité, intégrité, confidentialité, traçabilité
3. Ce que coûte un incident

03 Menaces et attaques

1. Qui attaque, et pourquoi
2. Les principales attaques
3. Vulnérabilités et chaîne d'attaque

04 Hameçonnage et ingénierie sociale

1. Reconnaître un message piégé
2. Fraudes au faux fournisseur et au président
3. Réagir et signaler

05 Analyser et traiter les risques

1. Du besoin de sécurité au scénario de risque
2. Évaluer et traiter un risque
3. Les méthodes de référence, à grands traits

06 Cadre juridique et acteurs de la cybersécurité

1. Les obligations de l'entreprise
2. Responsabilités, contrats et assurance
3. Les acteurs de la cybersécurité

07 Identités et accès

1. Mots de passe, phrases de passe et gestionnaire
2. Authentification multifacteur et comptes à privilèges
3. Gérer les droits : arrivées, départs, moindre privilège

08 Poste de travail, mobilité et usages d'Internet

1. Le poste de travail sous contrôle
2. Nomadisme et télétravail
3. Naviguer et échanger en sécurité

09 Sauvegarde, réseau, cloud et prestataires

1. Sauvegarder et pouvoir restaurer
2. Le réseau de l'entreprise, vu par un non-spécialiste
3. Cloud et prestataires : choisir et encadrer

10 Gérer un incident de sécurité

1. Détecter et qualifier un incident
2. Premiers gestes et cellule de crise
3. Après l'incident : déclarer, reprendre, apprendre

11 Piloter la sécurité : politique, sensibilisation et plan d'action

1. Politique de sécurité et charte informatique
2. Sensibiliser et faire adhérer
3. Le plan d'action de sécurité