PROGRAMME DE FORMATION

Cybersécurité -2 Sécurité de l'authentification

Cybersécurité & Protection des données

RÉFÉRENCE	VERSION	ÉDITION	DOMAINE
WF-0263	V2026-005	2 novembre 2026	Cybersécurité & Protection des données

DURÉE	MODALITÉ	PROGRAMME	SANCTION
1 h	Distanciel asynchrone (e-learning) · Présentiel	2 modules 2 leçons	Attestation et certificat de réalisation

Objectifs pédagogiques

Distinguer un mot de passe faible d'un secret robuste et construire une phrase de passe facile à retenir et difficile à deviner.

Appliquer la règle « un secret par service » à l'aide d'un gestionnaire de mots de passe et protéger en priorité la messagerie.

Reconnaître les situations qui exposent ses identifiants (fausse page de connexion, fuite, poste partagé, demande de mot de passe) et y réagir.

Choisir les comptes où activer en priorité l'authentification multifacteur et en préparer l'activation, codes de secours compris.

Établir son plan personnel de sécurisation des comptes et savoir quoi faire si un compte est piraté.

L'essentiel de la formation

Public visé

Tout salarié, quel que soit son service, travailleurs indépendants, dirigeants de très petites entreprises et toute personne qui veut protéger ses comptes professionnels et personnels (messagerie, banque, services en ligne) ; aucune compétence informatique particulière n'est attendue.

Prérequis

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

Aucun vrai mot de passe n'est demandé pendant la formation ; un traitement de texte permet de remplir le modèle de plan personnel fourni. Un positionnement en début de parcours situe votre point de départ.

Modalités et déroulement

Formation à distance, accessible en ligne, en une heure. Un court positionnement ouvre le parcours. Chaque leçon part d'une courte mise en situation vidéo dans une PME fictive, avec des personnages animés récurrents de la série « Cybersécurité » (un commercial itinérant, une assistante, un responsable informatique), puis fait pratiquer : tri de secrets fictifs, scénario à décisions, repérage d'erreurs et rédaction d'un plan personnel. Plus de la moitié du temps est consacrée à la pratique. Aucun vrai mot de passe n'est demandé ; aucune marque de logiciel n'est recommandée. Les bonnes pratiques ne sont jamais données de mémoire : chaque fiche méthode renvoie aux sources officielles (ANSSI, cybermalveillance.gouv.fr, CNIL) relues à la date de production. Accompagnement par un formateur par messagerie. Pour aller plus loin, des leçons du « Panorama SSI » (WF-0262) sont proposées en complément.

Méthodes pédagogiques

- Positionnement en début de parcours
- Apports en vidéo : explications et démonstrations
- Mises en situation et scénarios à décisions
- 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
- 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 tri, scénario et repérage d'erreurs ; règles de mots de passe et plan personnel vérifiés sur grille critériée ; quiz de module ; évaluation finale composée d'un cas court à décisions et d'un questionnaire. Seuil de réussite interne : 70 %.

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, fiches méthode et modèle 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 : **1 840 €**

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

2 modules, 2 leçons — durée totale 1 h.

01 Des mots de passe qui protègent vraiment

1. Phrases de passe et gestionnaire : un secret par service

02 Double authentification et compte piraté

1. Activer la double authentification et réagir à un compte piraté