AKADEMIA
FORMATION

PROGRAMME DE FORMATION
RÉF. N16

INTELLIGENCE ARTIFICIELLE | NIVEAU INITIATION

Cybersécurité et hygiène numérique *au quotidien.*

Une journée pour installer les réflexes qui protègent votre activité au quotidien : mots de passe et gestionnaire, double authentification, hameçonnage, mises à jour, sauvegardes, mobilité et données sensibles — fondés sur les recommandations de l'ANSSI et de Cybermalveillance.gouv.fr. Chacun part d'un autodiagnostic guidé, réalise trois actions de sécurisation en séance (gestionnaire installé, double authentification activée, sauvegarde vérifiée) et repart avec son plan d'hygiène numérique en dix actions et son kit de réflexes en cas d'incident.

DURÉE	FORMAT	PUBLIC	CERTIFICATION
1 jour	**Inter · Intra**	**Tous collaborateurs**	**Attestation**
7 heures	Présentiel ou distanciel		

À PROPOS DE LA FORMATION

Cybersécurité et hygiène numérique : les fondamentaux au quotidien.

Une journée pour installer les réflexes qui protègent votre activité au quotidien : mots de passe et gestionnaire, double authentification, hameçonnage, mises à jour, sauvegardes, mobilité et données sensibles — fondés sur les recommandations de l'ANSSI et de Cybermalveillance.gouv.fr. Chacun part d'un autodiagnostic guidé, réalise trois actions de sécurisation en séance (gestionnaire installé, double authentification activée, sauvegarde vérifiée) et repart avec son plan d'hygiène numérique en dix actions et son kit de réflexes en cas d'incident.

DURÉE	FORMAT	NIVEAU	PÉDAGOGIE	CERTIFICATION
1 jour	**Inter · Intra**	**Initiation**	**Active**	**Attestation**
7 heures	Présentiel ou distanciel		Petits groupes	Attestation délivrée

Objectifs pédagogiques

- Établir l'autodiagnostic de ses pratiques numériques (comptes et mots de passe, messagerie, double authentification, poste de travail, sauvegardes, mobilité, données) à l'aide d'une grille en langage courant fondée sur le guide d'hygiène informatique de l'ANSSI, et en déduire ses priorités personnelles.
- Créer et gérer des mots de passe robustes et uniques à l'aide d'un gestionnaire de mots de passe installé et amorcé en séance : phrase de passe maîtresse définie et comptes prioritaires migrés dans le coffre.
- Activer la double authentification sur au moins un compte prioritaire (messagerie, comptes administratifs ou bancaires), en choisissant la méthode adaptée — application d'authentification de préférence au SMS lorsque le service le permet — et en conservant ses codes de secours.
- Repérer un message d'hameçonnage à partir de ses signaux d'alerte (expéditeur, lien réel, pièce jointe, ton d'urgence, demande inhabituelle) et appliquer la procédure en trois gestes — ne pas cliquer, vérifier par un autre canal connu, signaler — y compris face aux variantes par SMS, par téléphone et à la fraude au virement.
- Appliquer au quotidien les mesures de protection du poste et des données : mises à jour automatiques activées, verrouillage de session, sauvegarde selon la règle 3-2-1 vérifiée en séance par un test de restauration, précautions en mobilité (wifi public, appareils, écrans) et séparation des usages professionnels et personnels, dans le respect des règles de partage des données sensibles.
- Dérouler les premiers réflexes face à un incident présumé : appliquer sa checklist personnalisée (isoler, préserver les preuves, ne pas payer ni dissimuler), alerter les bons interlocuteurs internes et mobiliser le dispositif public 17Cyber.
- Construire son plan d'hygiène numérique personnel et d'équipe — dix actions priorisées et planifiées, dont trois réalisées en séance — et personnaliser l'affichette de sensibilisation destinée à relayer les bons réflexes auprès de son équipe.

Public visé

Tous les collaborateurs, quels que soient le métier et le niveau de responsabilité : fonctions administratives et commerciales, accueil, production et ateliers, direction, fonctions support. La formation est conçue pour un public non technique : elle concerne aussi bien les équipes de TPE-PME sans service informatique dédié que les collaborateurs de structures équipées d'une DSI, ainsi que les managers souhaitant relayer les bons réflexes dans leur équipe grâce au kit remis (affichette de sensibilisation et checklist incident).

Prérequis

Aucun prérequis en cybersécurité ni en informatique au-delà de l'usage courant d'un ordinateur et d'une messagerie : la formation part de zéro et s'adresse à tous les collaborateurs. Chaque participant vient avec son ordinateur portable de travail, son téléphone mobile (nécessaire pour activer la double authentification) et ses identifiants d'accès à ses comptes principaux : les actions de sécurisation sont réalisées en séance sur SES propres outils. Une fiche de préparation transmise en amont permet de préparer les trois actions : installer avant la session l'application d'authentification recommandée sur son téléphone (ou signaler que le magasin d'applications est inaccessible) ; vérifier que l'on connaît — ou réinitialiser avant la session — les mots de passe actuels de ses trois comptes prioritaires ; indiquer si une sauvegarde existe déjà (espace entreprise, disque externe) et, à défaut, apporter un support ou obtenir du service informatique l'espace à utiliser ; enfin, lorsque le poste ou le mobile est administré par l'entreprise, obtenir la confirmation du service informatique (droits d'installation sur le poste, accès au magasin d'applications du mobile, double authentification autorisée sur la messagerie professionnelle). À défaut d'autorisation, un mode de travail alternatif est prévu en séance (démonstration guidée, puis action planifiée avec le service informatique).

PROGRAMME DÉTAILLÉ

Deux modules progressifs pour monter en compétences.

JOUR 1

Jour 1 — Des accès protégés au plan d'hygiène numérique

De l'autodiagnostic aux protections activées en séance, jusqu'au plan d'actions personnel et au kit de réflexes pour l'équipe.

MODULE

01.

3H30

Protéger ses accès : mots de passe, double authentification et hameçonnage

> **OBJECTIF OPÉRATIONNEL**
>
> *« Sécuriser ses accès sur SES propres comptes : autodiagnostic établi, gestionnaire de mots de passe installé et amorcé, double authentification activée sur un compte prioritaire, et réflexe anti-hameçonnage (repérer, réagir, signaler) entraîné sur des cas concrets. »*

CONTENU PÉDAGOGIQUE

- L'état de la menace, en chiffres sourcés et datés : en 2025, Cybermalveillance.gouv.fr a traité 504 000 demandes d'assistance (+20 % sur un an) ; pour les entreprises et associations, trois menaces dominent — le piratage de compte (21 % des parcours d'assistance, +52 %), l'hameçonnage (16 %) et la fraude au virement (13,5 %, +93 %) (rapport d'activité 2025, publié le 26 mars 2026). Lecture capacitante : selon l'ANSSI (guide d'hygiène informatique, 2017), la majeure partie des attaques ayant requis une intervention de l'agence aurait pu être évitée par des mesures d'hygiène élémentaires — celles de cette journée.
- Le référentiel de la journée : le guide d'hygiène informatique de l'ANSSI (42 mesures, v2.0 — septembre 2017), décliné à l'échelle du poste de travail et illustré par les chiffres et dispositifs récents ; pourquoi la sensibilisation de chaque collaborateur devient un standard : 80 % des TPE-PME s'estiment insuffisamment préparées (baromètre Cybermalveillance.gouv.fr et organisations patronales, octobre 2025), et la directive européenne NIS2 est en cours de transposition en France (à la date de conception, juillet 2026 : pas encore d'obligations françaises en vigueur).
- Autodiagnostic guidé de ses pratiques, sans jargon et sans jugement : comptes et mots de passe, messagerie, double authentification, équipements — la grille alimente directement le plan d'actions de fin de journée.

- Mots de passe : ce qui fait la robustesse (la longueur d'abord), pourquoi l'unicité compte autant (fuites de données massives et rejeu des mots de passe volés d'un site à l'autre), la phrase de passe facile à retenir ; le gestionnaire de mots de passe expliqué simplement — un coffre chiffré, un générateur, le remplissage automatique — et ce qu'il change au quotidien.
- Double authentification (aussi appelée validation en deux étapes ou MFA) : le principe — ce que je sais plus ce que je possède —, où l'activer en priorité (messagerie, comptes bancaires et administratifs, accès professionnels), application d'authentification de préférence au SMS lorsque le service le permet, codes de secours à conserver ; la règle absolue : un code de validation ne se communique jamais, à personne.
- Hameçonnage — repérer, réagir, signaler : les signaux d'alerte (expéditeur réel, lien caché derrière le texte, pièce jointe inattendue, ton d'urgence, demande inhabituelle) ; les trois gestes : ne pas cliquer, vérifier par un autre canal connu, signaler en interne et via les dispositifs officiels ; ce qu'aucun interlocuteur légitime ne demande jamais (mot de passe, code reçu par SMS).
- Les variantes du quotidien : hameçonnage par SMS et par téléphone, faux support technique, fraude au virement (faux fournisseur, changement de RIB, fausse urgence de la direction) — le réflexe qui protège : toute demande de paiement ou de changement de coordonnées bancaires se vérifie par un canal indépendant, systématiquement.

MISE EN PRATIQUE

Ateliers sur SES propres outils, en quatre temps : autodiagnostic guidé (volet comptes et messagerie) et choix de trois comptes prioritaires ; action 1 — installation du gestionnaire de mots de passe (solution de l'entreprise si elle existe, sinon solution gratuite proposée), création de la phrase de passe maîtresse et enregistrement des trois comptes prioritaires dans le coffre, dont au moins un mot de passe régénéré robuste et unique — la régénération des deux autres rejoint le plan d'actions ; action 2 — activation de la double authentification sur au moins un compte prioritaire, codes de secours conservés ; tri chronométré de huit messages « légitime ou piège » en binômes, correction collective et formalisation du réflexe en trois gestes.

LIVRABLE

Volet 1 de l'autodiagnostic renseigné ; gestionnaire de mots de passe installé et amorcé (phrase de passe maîtresse, trois comptes prioritaires enregistrés dans le coffre, dont au moins un mot de passe régénéré robuste et unique) ; double authentification activée sur au moins un compte ; mémo « trois gestes anti-hameçonnage » complété.

MODULE

02.

3H30

Protéger son poste et ses données, réagir à l'incident et bâtir son plan d'hygiène numérique

OBJECTIF OPÉRATIONNEL

« Protéger son poste et ses données au quotidien — mises à jour, sauvegarde vérifiée par un test de restauration, mobilité, données sensibles —, dérouler les premiers réflexes en cas d'incident, et consolider son plan d'hygiène numérique en dix actions avec le kit pour son équipe. »

CONTENU PÉDAGOGIQUE

- Un poste qui se défend presque seul : mises à jour automatiques du système et des applications (chaque mise à jour corrige des failles connues des attaquants), verrouillage de session, protections intégrées ; le cas des appareils en fin de support — exemple daté : depuis le 14 octobre 2025, Windows 10 ne reçoit plus de correctifs de sécurité par défaut ; les mises à jour de sécurité étendues (ESU) exigent une inscription, gratuite sous conditions pour les particuliers (compte Microsoft, jusqu'en octobre 2027) et payante pour les organisations (source Microsoft) — repérer ces appareils et les faire remonter.
- Sauvegardes : quoi sauvegarder, la règle 3-2-1 (trois copies, sur deux supports différents, dont une hors site ou hors ligne), sauvegarde automatique plutôt que manuelle, différence entre synchronisation et vraie sauvegarde avec historique ; le geste décisif : tester la restauration — une sauvegarde jamais testée n'est pas une sauvegarde.
- En mobilité et à la maison : wifi public et réseaux inconnus (préférer le partage de connexion de son téléphone), appareils verrouillés, discrétion des écrans dans les lieux publics, supports USB inconnus ; séparation des usages professionnels et personnels — messageries, comptes, stockage : pourquoi mélanger les deux expose l'entreprise comme le collaborateur.
- Les données sensibles au quotidien : repérer ce qui est sensible (données personnelles, RH, santé, éléments bancaires et contractuels), règles simples de stockage et de partage — espaces validés par l'entreprise plutôt que comptes personnels, destinataires vérifiés, droits d'accès limités — et le réflexe « ai-je le droit de l'envoyer, et par ce canal ? » (référence : guide CNIL de la sécurité des données personnelles, édition 2024).

- Réagir à un incident présumé — les premiers réflexes : isoler l'appareil du réseau, préserver les preuves (messages, captures d'écran), changer ses mots de passe depuis un appareil sain, alerter sans délai ; ce qu'il ne faut pas faire : payer une rançon, répondre au fraudeur, « nettoyer » ou réinstaller avant l'avis d'un professionnel, dissimuler l'incident ; qui prévenir : les interlocuteurs internes (service informatique, hiérarchie) et le dispositif public 17Cyber (17cyber.gouv.fr), guichet en ligne 24 h/24 lancé fin 2024 — diagnostic, conseils personnalisés et mise en relation avec un policier ou un gendarme.
- Fenêtre d'ouverture — ce que l'IA change déjà aux attaques : des leurres plus crédibles et personnalisés (textes soignés, voix clonées, vidéos truquées), produits plus vite et à plus grande échelle ; les fondamentaux de la journée restent la première parade — se méfier du contenu seul et vérifier par un autre canal ; panorama d'annonce, approfondi dans la formation N17 « Cybersécurité à l'ère de l'IA : phishing avancé, deepfakes et protection des données » (2 jours).
- Construire et faire vivre son plan d'hygiène numérique : consolidation de l'autodiagnostic, dix actions priorisées et planifiées (dont les trois réalisées en séance), affichette de sensibilisation personnalisée pour l'équipe, et ancrage dans la durée grâce aux ressources publiques gratuites référencées dans le répertoire remis (parcours SensCyber de Cybermalveillance.gouv.fr, guides ANSSI et CNIL).

MISE EN PRATIQUE

Ateliers sur SES propres outils : action 3 — vérification de sa sauvegarde par la restauration d'un fichier test (ou création d'une première sauvegarde), activation des mises à jour automatiques et volet 2 de l'autodiagnostic ; tri de cas « mobilité et données » (train, télétravail, clé USB trouvée, envoi d'un fichier RH) ; personnalisation de sa checklist incident (premiers gestes, contacts internes, numéros utiles) et finalisation de l'affichette d'équipe ; atelier final consacré au plan d'hygiène numérique — dix actions priorisées et planifiées, construites à partir de l'autodiagnostic — et tour de table d'engagement : chacun annonce son action n° 1 de la semaine.

LIVRABLE

Sauvegarde vérifiée et mises à jour automatiques activées ; autodiagnostic complet ; checklist « premiers réflexes en cas d'incident » personnalisée ; affichette de sensibilisation pour l'équipe ; plan d'hygiène numérique final en dix actions priorisées et planifiées.

MÉTHODES PÉDAGOGIQUES

Apprendre par la pratique, avec un formateur expert à vos côtés.

- Pédagogie active et apprentissage par le faire : la pratique occupe la place centrale — de l'ordre de 40 à 45 % du temps en atelier individuel accompagné où chacun sécurise réellement SES comptes et son poste (fil rouge), et plus de 60 % du temps consacré à la pratique au sens large en y ajoutant les démonstrations commentées, les tris de cas et le quiz ; le reste en apports courts et cadrés.
- Pédagogie positive et capacitante : chaque menace présentée est immédiatement suivie de la parade à la portée de tous ; aucun jargon non expliqué, aucune culpabilisation — on repart outillé, pas inquiet.
- Méthode magistrale : apports structurés courts, appuyés sur des supports visuels et sur des faits sourcés et datés (ANSSI, Cybermalveillance.gouv.fr, CNIL).
- Démonstrations en direct : le formateur manipule devant le groupe (gestionnaire de mots de passe, double authentification, test de restauration, parcours 17Cyber, lecture commentée de messages piégés) ; les démonstrations d'hameçonnage sont strictement pédagogiques, sur exemples anonymisés — jamais d'outil offensif ni de recette d'attaque.
- Méthode active : tri de messages « légitime ou piège » en binômes, tris de cas du quotidien, quiz interactif et restitutions favorisant l'ancrage des réflexes.
- Accompagnement individualisé : le formateur adapte le niveau de soutien selon le profil (à l'aise ou non avec l'outil informatique, poste administré ou non), sur la base du test de positionnement et de la fiche de préparation.
- Approche par compétences : chaque séquence aboutit à une action de sécurisation réalisée ou à un livrable directement réinvestissable.

Profil du formateur

Formateur expert à double compétence : sécurité numérique du quotidien (référentiels ANSSI, CNIL et Cybermalveillance.gouv.fr) et pédagogie des publics non techniques. Il justifie d'une expérience concrète de sensibilisation et d'accompagnement d'équipes non spécialistes (TPE-PME, collectivités ou services de grands comptes) et tient à jour sa veille sur l'état de la menace à partir des publications officielles datées. Sa veille couvre également l'évolution des attaques facilitées par l'IA (hameçonnage rédigé par IA, voix clonées), pour animer la fenêtre d'ouverture « ce que l'IA change déjà aux attaques » et orienter vers la formation N17.

Moyens & supports

- En présentiel : salle équipée d'un vidéo-projecteur, paperboard, connexion internet et wifi ; chaque participant travaille sur son propre ordinateur portable professionnel — les actions de sécurisation portent sur SES outils réels.
- En distanciel : classe virtuelle synchrone via les outils Akademia (partage d'écran, sous-groupes, partage de fichiers).
- Plateforme LMS Akademia (FormAI) : test de positionnement en ligne et mise à disposition de l'ensemble des ressources (supports, grille d'autodiagnostic, mémos pas-à-pas, jeu de messages d'entraînement, gabarits).
- Kit remis à chaque participant : grille d'autodiagnostic, mémos pas-à-pas (gestionnaire de mots de passe, double authentification, sauvegarde), checklist incident, affichette d'équipe et gabarit de plan d'hygiène numérique.
- Corpus pédagogique d'hameçonnage : messages réels anonymisés ou reconstitués à des fins d'entraînement, et extraits publics commentés pour la fenêtre « ce que l'IA change aux attaques » — aucun outil offensif n'est utilisé ni montré.

Modalités d'évaluation

- Test de positionnement en ligne réalisé sur la plateforme LMS avant le début de la formation (pratiques actuelles, aisance informatique), complété par un tour de table des attentes et, via la fiche de préparation, un état des droits d'installation sur le poste.
- Évaluation formative continue : chaque action de sécurisation réalisée en séance (gestionnaire installé, double authentification activée, sauvegarde vérifiée et mises à jour automatiques activées) est constatée par le formateur ; le tri de messages « légitime ou piège », les tris de cas et le quiz permettent de vérifier la progression objectif par objectif et d'apporter une remédiation immédiate.

- Ressources publiques de référence, présentées puis remises en répertoire : guide d'hygiène informatique de l'ANSSI, guide CNIL de la sécurité des données personnelles (édition 2024), dispositifs Cybermalveillance.gouv.fr (17Cyber, parcours SensCyber) pour prolonger la formation.

- Évaluation sommative : grille critériée d'atteinte des objectifs, renseignée au fil des ateliers puis consolidée et restituée en fin de journée, appliquée aux productions du fil rouge (autodiagnostic complété ; gestionnaire de mots de passe installé et amorcé ; double authentification activée ; sauvegarde vérifiée et mises à jour automatiques activées ; tri de messages « légitime ou piège » ; cas « mobilité et données sensibles » tranchés lors du tri de cas ; checklist incident personnalisée ; affichette d'équipe ; plan d'hygiène numérique en dix actions priorisées et planifiées), intégrant un critère d'usage responsable observable (le participant ne manipule que ses propres comptes, aucun mot de passe affiché ni partagé, aucune donnée sensible exposée pendant les exercices), complétée par un auto-positionnement de sortie reprenant les items du test amont pour objectiver la progression.
- Évaluation de satisfaction à chaud en fin de session et évaluation à froid à distance, à 1 à 3 mois, mesurant le transfert en situation de travail : actions du plan d'hygiène réalisées, réflexes appliqués (messages signalés, sauvegardes testées) et, lorsque le participant les communique, les retours de son équipe autour de l'affichette — à titre indicatif et non garanti.

Documentation remise aux stagiaires

- Le support de formation complet
- La grille d'autodiagnostic d'hygiène numérique (deux volets, fondée sur le guide ANSSI)
- Les mémos pas-à-pas illustrés : gestionnaire de mots de passe, double authentification, sauvegarde 3-2-1
- Le jeu d'entraînement « légitime ou piège » (huit messages anonymisés) et son corrigé commenté

Équipements à apporter

- Ordinateur portable
- Téléphone mobile (pour l'activation de la double authentification)

- Le mémo « trois gestes anti-hameçonnage » (modèle à compléter en séance)
- La checklist « premiers réflexes en cas d'incident » (modèle à personnaliser)
- L'affichette de sensibilisation pour l'équipe (modèle A4 à personnaliser)
- Le gabarit de plan d'hygiène numérique (dix actions priorisées et planifiées)
- Le répertoire des ressources publiques gratuites : 17Cyber, parcours SensCyber, guides ANSSI et CNIL
- Attestation de fin de formation mentionnant les objectifs et le résultat de l'évaluation des acquis

Accessibilité & handicap

Les besoins d'adaptation sont recensés dès l'inscription. Un référent handicap Akademia est identifié et joignable pour étudier, au cas par cas avec le participant, les aménagements possibles (rythme, supports, modalité). Les conditions d'accès sont vérifiées selon la situation.

Modalités & délais d'accès

Formation en petit groupe (4 à 6 participants), pour que chacun réalise en séance, sur ses propres outils, les trois actions de sécurisation — ou, lorsque la politique de sécurité de son entreprise l'impose, reparte avec chaque action préparée en démonstration guidée et planifiée avec son service informatique (mode alternatif prévu). Inscription en ligne ou auprès du service formation, entrée à date fixe selon le calendrier des sessions. Une fiche de préparation est transmise en amont (vérification des droits d'installation avec le service informatique, liste de ses comptes prioritaires). Pour les financements OPCO, l'inscription doit intervenir suffisamment tôt pour respecter les délais d'instruction du dossier ; Akademia accompagne le participant dans ses démarches.

Tarif

SESSION INTER-ENTREPRISES

890 € net de taxe

par participant · 1 jour (7 h)

Exonération de TVA · art. 261-4-4° a du CGI

SESSION INTRA-ENTREPRISE

Tarif sur devis

Session dédiée à vos collaborateurs, dans vos locaux ou à distance. Contactez-nous pour une proposition chiffrée personnalisée selon l'effectif et les modalités.

Prise en charge possible par votre OPCO ou France Travail. Nos équipes vous accompagnent dans le montage du dossier de financement.

PASSONS À L'ACTION

Construisons ensemble votre session sur-mesure.

Dites-nous vos contraintes (format, lieu, dates, nombre de participants) et recevez une proposition personnalisée sous 24 heures ouvrées.

Akademia Formation

SERVICE ADMINISTRATION DES VENTES

adv@akademiaformation.com

www.akademiaformation.com

Devis personnalisé

RÉPONSE SOUS 24 H OUVRÉES

Format inter · intra

Présentiel ou distanciel

FIN DU PROGRAMME