Sensibilisation à la cybersécurité

(Durée estimée : 3h)

Objectifs

- Comprendre les principaux enjeux de la cybersécurité et le rôle de chaque agent dans la protection du système d'information.
- Identifier les principales cybermenaces (phishing, ingénierie sociale, rançongiciels, usurpation d'identité, logiciels malveillants) et adopter les bons réflexes pour les éviter.
- Mettre en œuvre les bonnes pratiques de cybersécurité au quotidien : gestion des mots de passe, authentification multifacteur, navigation sécurisée, utilisation des équipements mobiles et protection des données.
- Réagir efficacement face à une situation suspecte en appliquant les procédures de signalement et les bonnes pratiques en cas d'incident.
- Adopter un usage responsable de l'intelligence artificielle, en identifiant ses opportunités, ses limites et les risques liés à la cybersécurité.
- Appliquer les principes essentiels du RGPD afin de protéger les données personnelles et respecter les obligations de confidentialité dans le cadre de leurs missions.

Contenu de la formation

Module 1 – Comprendre les enjeux de la cybersécurité

- Les cybermenaces aujourd'hui Pourquoi les collectivités territoriales sont des cibles privilégiées. Les principales cyberattaques observées ces dernières années. Les conséquences d'une attaque sur les services publics.
- Le rôle de chaque agent dans la sécurité du système d'information Les responsabilités individuelles.

Module 2 – Identifier les principales cybermenaces

- Le phishing Reconnaître un faux e-mail. Les faux SMS (smishing). Les appels frauduleux (vishing). Les faux sites Internet. Les QR Codes malveillants.
- Les logiciels malveillants Virus. Rançongiciels. Logiciels espions. Chevaux de Troie.
- L'ingénierie sociale Manipulation psychologique. Faux technicien informatique. Fraude au président. Usurpation d'identité.
- Atelier : analyse de véritables e-mails frauduleux et identification des indices d'une tentative d'attaque.

Module 3 – Les bonnes pratiques au quotidien

- Sécuriser son environnement numérique Choisir un mot de passe robuste. Utiliser un gestionnaire de mots de passe. Activer l'authentification multifacteur. Verrouiller son poste de travail. Réaliser les mises à jour.
- Utiliser les équipements mobiles en sécurité Les bonnes pratiques en télétravail. Les réseaux Wi-Fi publics. Les clés USB et supports amovibles.
- Que faire en cas d'incident ? Les bons réflexes. Qui contacter ? Pourquoi signaler rapidement est essentiel.

Module 4 – Intelligence artificielle, protection des données et RGPD

- L'intelligence artificielle : opportunités et vigilance Les usages actuels de l'IA générative. Les risques liés aux cyberattaques utilisant l'IA : E-mails de phishing plus crédibles. Imitation de voix et de vidéos (deepfakes). Création de faux documents. Démonstration d'un exemple concret d'utilisation de l'IA pour illustrer les nouvelles formes de fraude.
- Les bonnes pratiques avec les outils d'IA Quelles informations ne jamais saisir dans une IA publique. Différence entre données publiques, internes, confidentielles et personnelles. Vérifier les réponses produites par une IA. Respecter les consignes de la collectivité concernant l'utilisation des outils d'IA.
- Protection des données personnelles (RGPD) Comprendre ce qu'est une donnée personnelle. Les obligations de confidentialité des agents. Les risques liés au partage de données. Les bons réflexes pour protéger les informations des usagers et des collègues. Exemples concrets de situations rencontrées dans une collectivité.

Module 5 – La cybersécurité au quotidien… même à la maison

- Parce que les mêmes réflexes permettent également de protéger sa famille.

Campus26 Cité numérique du Pensio - 4 rue du PNDF - 43000 Le Puy-en-Velay - 0415490003 - www.campus26.com - contact@campus26.com
SARL capital 50 000€ - SIRET : 82253076200027 - APE : 6201Z - TVA intra : FR 838 225 307 62 - N° OF : 844 303 392 43

- Sécuriser son smartphone.
- Les achats en ligne.
- Les arnaques bancaires.
- Les réseaux sociaux.
- Sauvegarder ses photos et documents.
- Protéger les comptes de ses proches.

Moyens pédagogiques

- Présentation interactive.
- Nombreux exemples réels.
- Démonstrations.
- Quiz en direct.
- Analyse collective de situations.
- Questions/réponses.
- Fiche mémo 'Les 10 réflexes cybersécurité'.

Moyens techniques

- Salle de formation équipée d'un vidéoprojecteur ou d'un écran de diffusion.
- Ordinateur du formateur avec connexion Internet.
- Support de présentation (PowerPoint ou équivalent).
- Démonstrations en direct de situations de phishing et de bonnes pratiques de cybersécurité.
- Quiz interactif accessible via smartphone (QR Code) ou ordinateur.
- Supports pédagogiques remis aux participants (version numérique).
- Tableau blanc ou paperboard pour les échanges et la synthèse.

Modalités d'encadrement

La formation est animée par un formateur spécialisé en cybersécurité et en sensibilisation aux usages numériques.
L'intervenant alterne apports théoriques, exemples concrets, démonstrations et échanges avec les participants afin de favoriser l'acquisition des bonnes pratiques.
La formation peut être réalisée :

- En présentiel : animation en salle avec interactions directes, mises en situation et échanges collectifs.
- En classe virtuelle : animation en visioconférence avec partage d'écran, démonstrations en direct, utilisation d'outils interactifs (quiz, sondages, chat) et temps dédiés aux questions des participants.

Le formateur adapte le rythme et le niveau des explications au public afin de favoriser la participation et la compréhension des notions abordées. Les participants peuvent poser leurs questions tout au long de la formation.

Evaluation des acquis

- Quiz envoyé avant la formation pour mesurer les connaissances initiales.
- Questions interactives tout au long de la formation.
- Quiz final de validation des acquis.

Pré-requis

Aucun prérequis technique n'est nécessaire.
Cette formation est accessible à toute personne utilisant un ordinateur, une messagerie électronique ou des outils numériques dans le cadre de son activité professionnelle.
Pour la participation en classe virtuelle, les participants doivent disposer :

- D'un ordinateur équipé d'une connexion Internet stable.
- D'un navigateur web à jour.
- D'un casque ou de haut-parleurs (un microphone est recommandé afin de faciliter les échanges).

Public visé

Cette formation s'adresse à l'ensemble des agents des collectivités territoriales, quels que soient leur service ou leur fonction, utilisant un ordinateur, une messagerie électronique, Internet ou des applications métiers dans le cadre de leurs missions. Elle est destinée en priorité à un public débutant ou ayant peu de connaissances en cybersécurité (niveau initiation). Les contenus sont volontairement accessibles, sans vocabulaire technique, et centrés sur l'acquisition des bons réflexes face aux principales menaces numériques du quotidien.

Tarif

600 € HT pour un groupe de 1 à 12 personnes
Tarif indicatif. Nous consulter pour un devis personnalisé.

Modalités d'accès

INTRA entreprise

Délais d'accès

1 jour(s) ouvré(s)

Accessibilité

Formation accessible aux personnes à mobilité réduite en présentiel ou en classe virtuelle. Pour plus de précision, nous contacter.

Cette formation est récente : les indicateurs de résultats seront publiés à l'issue des premières sessions.

Ouverte depuis le 02/11/2026

Indicateurs mis à jour le 4 novembre 2026.

Contact

Campus26 — Cité numérique du Pensio, 4 rue du PNDF, 43000 Le Puy-en-Velay
Téléphone : 04 15 49 00 03
Courriel : contact@campus26.com

Mise à jour du programme : 04/11/2026