FORMATION - FORMATION - SÉCURITÉ NUMÉRIQUE : PROTÉGER SES DONNÉES ET SES COMMUNICATIONS

Public et pré-requis
Journaliste, documentaliste, communicant·e, élu·e en collectivité territoriale, enquêteur·trice, militant·e, responsable associatif, défenseur des libertés numériques ou simplement intéressé·e par le sujet.
Aucun prérequis de niveau.

Durée et modalités pédagogiques
Formation Présentiel de 14h

Moyens pédagogiques
Le support numérique de formation vous est transmis pendant ou après la session.

Accessibilité
Nous mettons tout en œuvre pour vous accueillir toutes et tous dans les meilleures conditions. Notre charte handicap détaille nos engagements pour l'accessibilité de nos formations. Contactez notre référent handicap si vous avez des besoins spécifiques d'accompagnement avant, pendant et après la formation: handicap@samsa.fr

Evaluation
1- Positionnement
Un questionnaire en ligne est adressé aux participant·e·s avec la convocation de manière à évaluer leur niveau initial et leurs attentes.
2-Evaluation des acquis
Au cours de la formation, les exercices réalisés permettent au formateur ou à la formatrice d'évaluer l'acquisition des compétences.
3- Attestation
Une attestation des acquis de fin de formation est adressée par mail aux apprenants suite à la session

Matériel
Un ordinateur ayant un accès internet.

Dernière modification contenu formation - 20/04/2026

Objectifs

- Comprendre et prévenir les attaques en ligne
- Sécuriser votre matériel (ordinateur, smartphone)
- Manipuler et adopter des outils opérationnels au quotidien
- Mettre en place des réflexes dans votre navigation sur internet
- Travailler sur le web de manière sécurisée
- Protéger vos sources grâce à des communications sécurisées
- Stocker vos informations de manière sécurisée
- Contribuer à la sécurité collective de votre organisation

Programme

Jour 1

Matin : les bases de la sécurité numérique

- Présentation de la formatrice et tour de table pour identifier les attentes
- Présentation des différents types de menaces informatiques
- Tour d'horizon des comportements à risques avec un ordinateur ou un smartphone
- Évaluation des risques pour chaque participant
- Présentation des sécurités de base sur un ordinateur et un téléphone
- Mise en place des sécurités sur les ordinateurs et téléphones de chaque participant
- Conseils pour mettre en place de bonnes pratiques dans son entourage

Après-midi : protéger sa navigation et son investigation en ligne

- Vérification des paramètres de sécurité sur les réseaux sociaux pour chaque membre de l'équipe
- Vérification de la gestion individuelle et collective des mots de passe
- Comprendre la navigation sur Internet et les points d'interception du trafic
- Faire des recherches sur internet de manière sécurisée
- Adopter des solutions contre l'interception de données

Jour 2

Matin : protéger ses communications en ligne

- Rappel juridique sur le secret des sources
- Le modèle de menace en 5 questions
- Connaître et identifier les menaces informatiques
- Présentation d'outils et services pour communiquer de manière anonyme et/ou chiffrée sur smartphone et sur ordinateur

FORMATION - FORMATION - SÉCURITÉ NUMÉRIQUE : PROTÉGER SES DONNÉES ET SES COMMUNICATIONS

- Conseils pour transmettre de bonnes pratiques à ses sources/interlocuteurs

Après-midi : stocker ses données en toute sécurité

- La légalité des outils de chiffrement selon les pays
- Local ou cloud : comment sauvegarder ses données ?
- Comparaison des outils de cloud les plus répandus (Google drive, Onedrive, WeTransfer, Spider oak)
- Apprendre à chiffrer un fichier, un répertoire, un disque dur avec VeraCrypt
- Éliminer les infos sensibles dans ses fichiers : apprendre à lire les métadonnées avec ExifViewer
- Rappel des points importants
- Évaluation à chaud de la formation par les participants