RéflexesNumériques

SIRET N° 53209667400025
https://www.reflexesnumeriques.fr
contact@reflexesnumeriques.fr
Version du 03/06/2026

Cybersécurité et Hygiène Numérique

Objectifs de la formation :

✓ **Comprendre les enjeux de la cybersécurité et les risques actuels.**
✓ **Reconnaître les attaques courantes et les tentatives d'escroquerie.**
✓ **Mettre en place de bonnes pratiques simples et efficaces.**
✓ **Savoir quoi faire en cas d'incident ou de cyberattaque.**

- **Durée : 7 heures**
- **Public :** particuliers, indépendants, TPE/PME, collectivités.
- **Pré-requis :**
  - Utilisation d'un ordinateur.
  - Connexion internet et logiciel de visio conférence (zoom, skype…) dans le cas d'une formation à distance

Méthodologie :
- Formation en présentiel ou à distance.
- présentation théorique des sujets
- Exemples pratiques

Modalités/délais d'accès:
- Entretien téléphonique, validation dossier
- délai 14 jours de réflexion

Moyens et méthodes pédagogiques :
- Active et démonstrative
- Images d'exemples pour exercices fournies
- Supports de cours remis en fin de formation.
- Formateur expérimenté.

Evaluation de la formation :

- évaluation en continu avec exemples pratiques

Accessibilité handicap :
Nous contacter pour analyse et proposition de solutions en fonction de votre situation.

Dates : A planifier avec le formateur.

Programme :

1. Comprendre la cybersécurité
- Pourquoi la cybersécurité est devenue essentielle.
- La défense en profondeur.
- Disponibilité, Intégrité, Confidentialité (DIC).
- Conséquences d'un incident de sécurité.
- Impacts financiers, juridiques et réputationnels.

2. Identifier les cybermenaces et se protéger
- Phishing, smishing, quishing et vishing.
- Vol d'identifiants.
- Mots de passe et authentification.
- Logiciels malveillants et rançongiciels.
- Menaces internes et erreurs humaines.
- Attaques de la chaîne d'approvisionnement.

3. Sécuriser son environnement numérique
- Recadrer, redresser les images
- Sauvegardes et méthode 3-2-1.
- Sécurisation des appareils mobiles.
- Introduction aux gestionnaires de mots de passe.
- Double authentification (2FA).
- IA générative et protection des données.
- Sensibilisation RGPD et données personnelles.

4. Réagir à une cyberattaque
- Premiers réflexes.
- Isolation des équipements compromis.

- Communication et gestion de crise.
- Notification CNIL.
- Retour d’expérience et amélioration continue.