



## PUBLIC

Tout public voulant se sensibiliser aux usages du numérique



## PRÉ-REQUIS

Aucun



## DURÉE

1 jour - 7 heures



## MODALITÉS

Présentiel



## TYPE DE VALIDATION

Certificat de réalisation

Attestation de fin de formation

## » CONTEXTE

- Depuis les années 2000, Internet a transformé les modalités d'accès et de diffusion de l'information. En devenant social et interactif, le Web a pris une place de plus en plus importante dans notre quotidien, tant sur le plan personnel que sur le plan professionnel. Très positive par certains aspects, cette évolution génère également de nouveaux comportements à risque et de nouveaux dangers.

## » RÉSULTATS ATTENDUS

- Prendre conscience des dangers du Web et des réseaux sociaux, apprendre à repérer les conduites à risques et à adopter les bonnes pratiques pour prévenir les dangers.

## » OBJECTIFS PÉDAGOGIQUES

- Identifier les différents dangers liés au Web et aux réseaux sociaux
- Mesurer les conséquences des pièges tendus sur le Web et les réseaux sociaux
- Adopter les bonnes pratiques pour limiter les risques
- Repérer les outils dédiés à la lutte contre les dangers du Web et des réseaux sociaux
- Adapter son comportement pour se protéger
- Adapter son comportement pour protéger son entourage
- Agir pour se défendre et pour protéger les autres

## » MÉTHODES PÉDAGOGIQUES

- Méthode active et participative.
- Une approche réflexive pour analyser ces pratiques de chacun.
- Remise d'un livret pédagogique reprenant en synthèse les trois axes de travail : définition des dangers liés au Web et aux réseaux sociaux, rappel des bonnes pratiques et rappel des règles de sécurité.



## DATES ET LIEUX

A Définir - dans vos locaux



## TARIFS

NOUS CONSULTER



## INTERVENANT

Nicolas GAUGUELIN  
Formateur auprès de public  
travailleurs en situation de  
handicap



Lieux aménagés et modalités adoptées pour faciliter l'accès et l'usage aux personnes en situation de handicap.

## PROGRAMME

### IDENTIFIER LES DIFFERENTS DANGES LIES AU WEB ET AUX RESEAUX SOCIAUX, ET EN COMPRENDRE LES MECANISMES

- Qu'est-ce que le hacking ? (Virus, vol des données personnelles, usurpation d'identité)
- Qu'est-ce que le phishing ? (Par e-mail ou via les réseaux sociaux, en particulier les messageries)
- Quels sont les différents aspects du cyber-harcèlement ? (Verbal, moral, à caractère sexuel)
- Prendre conscience de la persistance dans le temps des contenus diffusés (diagnostic d'e-réputation, impacts et enjeux pour la vie personnelle et la vie professionnelle)
- Prendre conscience du complotisme et comprendre le mécanisme des manipulations (*fake news*)

### ADOPTER LES BONNES PRATIQUES, REPERER LES OUTILS ESSENTIELS

- Protéger ses données personnelles
- Régler les paramètres de confidentialité (comprendre les interactions entre domaine public et domaine privé)
- Connaître les membres de sa communauté (définir un degré de confiance, comprendre qu'il existe de fausses identités, bloquer les comptes suspects)
- Connaître et respecter la loi (diffamation, injures raciales, incitation à la haine, attentat à la pudeur)
- Régler les filtres de contenus et commentaires à caractère offensants
- Identifier la source d'une information

### ADAPTER SON COMPORTEMENT

- **Se protéger :**
  - ✓ Choisir des mots de passe efficaces et penser à se déconnecter en fin de session
  - ✓ Ne pas divulguer ses identifiants (mots de passe, numéro de sécurité sociale, accès aux comptes bancaires...)
- **Protéger son entourage :**
  - ✓ Ne pas diffuser les informations personnelles de personnes tierces
  - ✓ Ne pas relayer des informations dont on ne connaît pas la source
- **Agir pour se défendre et pour protéger les autres :**
  - ✓ Signaler les contenus inadaptés (diffamation, injures raciales, incitation à la haine, contenus à caractère pornographique)
  - ✓ Victime ou témoin de cyber-harcèlement : parler, ne pas s'isoler, connaître les recours