# Initiation à la sécurité informatique

## Modalités pédagogiques

**Objectif** : Comprendre les enjeux de sécurité liés à l'usage de l'informatique, savoir identifier les principales menaces, acquérir les réflexes de bonnes pratiques afin de se protéger et protéger son entreprise.

**Type de public** : Tout utilisateur des outils numériques souhaitant s'initier à la sécurité informatique afin de mieux prendre conscience des comportements à risque et acquérir les bons réflexes

**Pré-requis** : Etre familier des outils numériques : ordinateur, smartphone, internet, emails…

**Moyens pédagogiques** : présentation au vidéoprojecteur, support de cours remis aux stagiaires, exercices pratiques, études de cas tout au long du stage

**Evaluation des acquis** : à chaud, sous forme d'exercices pratiques

## Modalités d'exécution

**Durée** : 1 jour, 7 heures

**Dates** : à définir ultérieurement selon nos disponibilités mutuelles

**Lieu** : Rhône/Loire, sur site client ou salle extérieure, à définir ultérieurement (cf. option sur devis)

**Formateur** : Aurélie DUSONCHET, spécialiste informatique et bureautique

**Nombre de participants** : 2 à 8 stagiaires

**Modalités de suivi** : feuille d'émargement, attestation de formation individuelle

**Tarif** : 590 € HT / participant (tarifs intra : nous consulter)

## Programme pédagogique détaillé

**Objectifs et enjeux**

- Que veut-on protéger et pourquoi ?
  - Nos données sont importantes
  - Nos données sont vulnérables
- Que craignons-nous ? : typologie des risques
  - Disponibilité
  - Intégrité
  - Confidentialité
  - Traçabilité

**Les types de menaces**

- Des motivations diverses
- Menaces de masse
  - Phishing
  - Ddos
  - Botnet
  - Ransomwares et cryptowares
  - Ver, virus, spyware, trojan
- Menaces ciblées
  - cyberespionnage (économique, industriel)
  - APT
  - vol d'identité

**Les moyens de protection**

- sauvegardes
- outils informatiques spécifiques
  - antivirus
  - pare-feu

**Les règles de bonnes pratiques**

- mises à jour
- mots de passe
- téléchargement
- e-mails
- réseaux wifi
- smartphones et tablettes
- BYOD
- déplacements
- paiement en ligne
- protéger son identité numérique

**Que faire en cas d'attaque ?**

- stopper l'attaque : les bons réflexes
- informer
- rechercher des preuves
- tirer les leçons