# Prévention des risques et sécurité informatique

## Programme de formation

**Objectifs :**

- Comprendre les enjeux de la sécurité informatique et les tendances actuelles des attaques
- Développer la capacité à reconnaître et à contrer les tentatives de phishing
- Avoir des comportements sécurisés à la maison, au travail et en déplacement
- Comprendre l'importance des mots de passe et apprendre à les utiliser de manière appropriée
- Se familiariser avec les outils de sécurité informatique

**Durée :**
1 journée soit 7 heures

**Public :**
Toute personne ayant accès à du matériel connecté ou informatique

**Prérequis :**
Aucun

**Moyens et outils pédagogiques :** Vidéoprojecteur, Paperboard ou tableau blanc, Quizz, Jeux de rôles

**Nombre de formateurs :** 1

**Lieu et date :** en présentiel

**Coût :** à partir de 860 € HT (soit 1032 € TTC)

*A l'issue de la formation chaque participant recevra un certificat de réalisation, un livret de formation, un questionnaire de satisfaction et un questionnaire de validation des acquis*

**AJ Consulting s'engage à rendre ses formations accessibles aux personnes en situation de handicap. N'hésitez pas à contacter notre référent handicap pour discuter de vos besoins spécifiques.**

**AJ Consulting**
Conseil – Audit – Formation
27 rue Jean Jaurès – 29120 Pont l'Abbé
Tél : 02 22 94 12 21
SIRET : 511 588 295 00028 – APE 6202A – NDA 53 29 10088 29 – TVA FR 515 511 588 295

# Déroulé de la formation

## Module 1 : introduction à la sécurité informatique

*Objectif : Comprendre les enjeux de la sécurité informatique et les tendances actuelles des attaques.*

- Introduction de la formation, présentation du formateur et des apprenants
- Présentation des grandes tendances en termes d'attaques récentes
- Sensibiliser aux risques pour les individus et les entreprises
- Exploration des 3 principaux types de pirates informatiques
- Définition et exemples d'ingénierie sociale et des techniques utilisées par les attaquants pour manipuler les utilisateurs

## Module 2 : identifier

*Objectif : Développer la capacité à reconnaitre et à contrer les tentatives de phishing*

- Explication du concept de phishing / exemples concrets
- Identifier les signaux d'alerte – reconnaitre une tentative de phishing
- Les 5 règles d'or pour ne pas tomber dans le piège

## Module 3 : adopter les bons comportements

*Objectif ; Promouvoir des comportements sécurisés à la maison, au travail, en déplacement*

- Les bonnes pratiques pour sécuriser son environnement domestique et professionnel
- Les risques potentiels des lieux publics, conseils pour minimiser les risques lors des déplacements
- Sensibilisation à la sécurité des dispositifs physiques (supports amovibles, Smartphone, objets connectés…)

## Module 4 : se protéger

*Objectif : comprendre l'importance des mots de passe et apprendre à les utiliser de manière sécurisée*

- L'importance d'avoir un bon mot de passe : les conséquences d'un mot de passe faible
- Critères pour créer un mot de passe fort et sécurisé
- Astuces pour créer et retenir facilement un mot de passe complexe
- Le bon usage d'un mot de passe
- Les gestionnaires de mots de passe
- Le futur ? L'authentification multi facteurs

## Module 5 : les outils disponibles pour renforcer sa sécurité

*Objectif : Familiariser les participants avec les outils de sécurité informatique*

- Les antivirus : leur rôle, leurs limites, choisir un antivirus qui convient à ses usages
- Les pares-feux : leur rôle dans la sécurité du réseau, la différence entre pares-feux matériels et logiciels, les configurations recommandées suivant ses pratiques
- Le Cloud ses avantages, ses risques