

## PROGRAMME DE FORMATION

### Hygiène numérique et sensibilisation à la cybersécurité

#### OBJECTIFS PEDAGOGIQUES

A l'issue de la formation l'apprenant sera capable de :

- Reconnaître les différents risques liés à la cybersécurité
- Comprendre les méthodes et outils des pirates informatiques
- Repérer et réagir à des mails de phishing sophistiqué
- Comprendre le piratage psychologique et comment y faire face
- Maîtriser des outils et méthodes pour faire face aux différents vecteurs d'attaques informatiques

**Profil des stagiaires :** Salarié d'entreprise ou agent de collectivité utilisant quotidiennement un ordinateur

**Prérequis :** Utiliser quotidiennement des outils numériques (ordinateur, smartphone, navigateur web etc.)

**Durée :** 7 heures ( 1.00 jour)

**Date :** A fixer avec le formateur / Accessibilité sous 2 semaines

**Modalité d'accès :** Entretien téléphonique pour connaître et analyser les besoins

**Modalités pédagogiques :** Formation présentielle

**Coût :** Nous consulter pour un devis

#### CONTENU DE LA FORMATION

- Introduction et Échanges :
  - Présentation des participants : parcours, profils, niveaux d'expérience.
  - Discussion sur l'exposition individuelle aux risques cyber.
- Définition de l'Hygiène Numérique :
  - Explication des concepts clés : qu'est-ce que l'hygiène numérique ?
- Prise de conscience des Risques :
  - Identification des risques numériques selon le profil (PME, grande entreprise, organisme public, individu).
- Comprendre les Méthodes des Attaquants :
  - Mise en situation ludique pour appréhender les techniques et outils des attaquants et apprendre à s'en défendre.
- Détection des mails de Phishing :
  - Savoir identifier les éléments suspects dans un mail.
  - Réactions appropriées face à un e-mail de phishing.
- Piratage Psychologique :
  - Sensibilisation à l'exploitation de la psychologie humaine par les attaquants.
  - Techniques pour détecter et se prémunir contre ces attaques.
- Gestion des Identifiants Numériques :
  - Utilisation des outils appropriés pour une gestion sécurisée des identifiants.

#### ORGANISATION DE LA FORMATION

**Moyens et méthodes pédagogiques :**

- Accueil des stagiaires dans une salle dédiée à la formation.
- Documents supports de formation projetés
- Jeu de mise en situation « Dans la tête dans un hacker »
- Approche ludique
- Exposés théoriques
- Formateur expert en cybersécurité

**Dispositif de suivi de l'exécution de l'évaluation des résultats de la formation :**

- Questions orales tout au cours de la formation
- QCM à la fin de la formation
- Mises en situation
- Certificat de réalisation

**Accessibilité aux personnes en situation de handicap**

N'hésitez pas à nous contacter. Nous analyserons avec vous la meilleure formule de formation adaptée à votre situation.

Retrouvez plus d'informations sur l'accès à la formation pour les personnes en situation d'handicap sur les sites de l'Agefiph, les Cap emploi, du Fiphfp ou des MDPH.

Ce programme sera adapté en fonction des niveaux et des attentes de chaque participant. Des moyens de compensation seront mis en place pour les personnes en situation de handicap.

**Contacts**

Téléphone : 06 87 06 18 35

Email : [contact-pro@victorprouff.fr](mailto:contact-pro@victorprouff.fr)