V1CT0R PR0UFF
Formation

26 janvier 2026

PROGRAMME DE FORMATION

Cybersécurité : Comprendre pour mieux se protéger - 1/2 journée

OBJECTIFS PEDAGOGIQUES

À 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 ;
- comprendre l'ingénierie sociale et comment y faire face ;
- repérer et réagir à des mails de phishing sophistiqué ;
- maîtriser des outils et méthodes pour faire face aux différents vecteurs d'attaques informatiques.

Profils des stagiaires : Dirigeant d'entreprise, indépendant, cadre utilisant quotidiennement un ordinateur.

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

Durée : 3,5 heures (1/2 journée).

Date : à fixer avec le formateur / Accessibilité sous 2 semaines.

Modalité d'accès : entretien téléphonique pour connaître et analyser les besoins.

Modalités pédagogiques : formation présentielle.

Coût : devis sur-mesure en fonction du nombre d'apprenants et de la localisation.

CONTENU DE LA FORMATION

- Introduction et Échanges :
  - présentation des participants : parcours, profils, niveaux d'expérience ;
- Prise de conscience des risques :
  - identification des risques numériques selon le profil (PME, grande entreprise, organisme public, particulier) ;
  - En quoi les PME sont des cibles privilégiées ?
- Les méthodes utilisées par les cybercriminels
  - Les attaques opportunistes :
    - fuites de données ;
    - phishing ou mails frauduleux ;
    - Ransomware ou rançongiciel ;
    - Les failles de sécurité logicielles.
  - Les attaques ciblées :
    - OSINT – Recherche sur Sources ouvertes ;
    - l'ingénierie sociale, sensibilisation à l'exploitation de la psychologie humaine.
  - L'intelligence artificielle, ce qu'elle apporte aux cybercriminels.
- Les solutions : méthodes et outils pour se protéger.
  - Que faire en cas d'attaque ?
  - Prévenir et limiter les risques :
    - gérer ses identifiants numériques (gestionnaire de mots de passe, double authentification) ;
    - détecter des mails/sms de Phishing ;
    - se prémunir des attaques par ingénierie sociale ;
    - rôles, responsabilité et process ;
    - les incontournables de la sécurité.

ORGANISATION DE LA FORMATION

Moyens et méthodes pédagogiques :

- accueil des stagiaires dans une salle dédiée à la formation ;
- documents supports de formation projetés ;
- 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 court 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
E-mail : contact-pro@victorprouff.fr