INQUEST CYBERSÉCURITÉ

CGPA CAMPUS

FICHE FORMATION

PROTEGER SON **IDENTITE NUMERIQUE**

Formation visant à sensibiliser les participants à protéger leurs identités numériques

1h | **e-learning** | **Agents, courtiers, IOBSP et leurs collaborateurs.** | **Cybersécurité**

Informations générales

- Prérequis : **Sans objet**
- Niveau : **Débutant**
- Délais d'accès : **Dès l'inscription**
- Modalités d'accès : **Après inscription, un mail de CGPA Campus vous invitera à rejoindre la plateforme. Le lien restera valable 2 mois.**
- Durée d'accès : **Les apprenants peuvent revoir la formation en ligne autant de fois que souhaité durant sa période d'accès.**
- Domaine : **Informatique**
- Sous-domaine : **Cybersécurité**
- Spécialité : **Sécurité informatique**
- Accès PSH : N/A
- Tarif : **offert aux sociétaires CGPA**

Objectifs de formation

- Identifier les risques d'exposition (réseaux sociaux, empreinte numérique).
- Comprendre les techniques : OSINT, spearphishing, fraude au président, ingénierie sociale.
- Reconnaître les vecteurs d'attaque et les erreurs humaines fréquentes.
- Adopter des bonnes pratiques concrètes (paramétrage confidentialité, vigilance face aux mails urgents, gestion mots de passe, sensibilisation collègues).
- Savoir auditer et nettoyer son empreinte numérique.
- Vérifier ses acquis avec un quiz.

Critères de réussite

Une attestation est délivrée dès 70 % de bonnes réponses, téléchargeable immédiatement dans « Mes cours ». Les Apprenants seront invités à remplir un questionnaire de satisfaction permettant d'évaluer l'e-learning suivi et la fiche récapitulative sera disponible et téléchargeable sur la plateforme de formation.

Séquençage pédagogique

Nombre de parties : 9

1. Identité numérique : Quels sont les risques
2. Introduction – Dans la peau d'un attaquant
3. Étape 1 – Collecte d'informations (OSINT)
4. Étape 2 – Ingénierie sociale & mots de passe faibles
5. Étape 3 – Spearphishing & fraude au président
6. Empreinte numérique : ce que dit Google de vous
7. Les bonnes pratiques
8. Quiz final
9. Fiche récapitulative

Méthodes pédagogiques

- Scénarisation immersive ("dans la peau d'un attaquant").
- Études de cas et mises en situation (LinkedIn, Facebook, phishing, fraude).
- Activités interactives : glisser-déposer, quiz intermédiaires, vrai/faux. Fiche
- récapitulative finale.

Modalités d'évaluation

Quiz évaluation.

FICHE FORMATION

PROTEGER SON **IDENTITE NUMERIQUE**

Formation visant à sensibiliser les participants à protéger leurs identités numériques

Séquençage du module

Seq.1 : Identité numérique : Quels sont les risques ?

Seq.2 : Introduction – Dans la peau d'un attaquant

Seq.3: Étape 1 – Collecte d'informations (OSINT

Seq.4 : Étape 2 – Ingénierie sociale & mots de passe faibles

Seq.5 : Étape 3 – Spearphishing & fraude au président

Seq.6 : Empreinte numérique : ce que dit Google de vous

Seq. 7 : Les bonnes pratiques

Seq. 8 : Quiz final

Seq. 9 : Fiche récapitulative (PDF téléchargeable)

Outils

- Plateforme LMS
- Support de cours
- Questionnaire d'évaluation QCM

Date

- 1er novembre 2025