INQUEST CYBERSÉCURITÉ

CGPA CAMPUS

FICHE FORMATION

SENSIBILISATION A LA **CYBERSECURITE**

Formation visant à sensibiliser les participants à la cybersécurité

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

- Comprendre l'ampleur de la menace cyber (données chiffrées, typologie attaquants).
- Identifier le phishing et ses déclinaisons (mails, liens, faux sites).
- Savoir réagir face à une tentative de phishing.
- Adopter des bonnes pratiques concrètes au bureau (poste de travail, bureau propre).
- Connaître les risques liés aux périphériques (clés USB).
- Appliquer les bons réflexes en télétravail.
- Intégrer la DSI comme acteur clé de la sécurité.
- Consolider ses acquis via un quiz final.

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 : 13

1. Présentation du module
2. État de la cybermenace
3. Qu'est-ce que le phishing
4. Comment repérer une tentative de phishing
5. Différence http / https
6. Comment repérer un lien malveillant
7. Que faire en cas de phishing
8. Politique du bureau propre
9. Pourquoi les clés USB ont mauvaise presse
10. Cybersécurité & télétravail
11. Besoin d'un logiciel ? La DSI est mon amie !
12. Quiz final
13. Fiche récapitulative

Méthodes pédagogiques

- Cas pratiques et mises en situation (ex. mails frauduleux, liens suspects).
- Activités interactives : glisser-déposer, vrai/faux, associations.
- Visualisations chiffrées (statistiques cyberattaques).
- Fiche récapitulative téléchargeable.

Modalités d'évaluation

Quiz évaluation.

INQUEST CYBERSÉCURITÉ

CGPA CAMPUS

FICHE FORMATION

SENSIBILISATION A LA **CYBERSECURITE**

Formation visant à sensibiliser les participants à la cybersécurité

Séquençage des modules

Seq.1 : Présentation du module

Seq.2 : État de la cybermenace

Seq.3 : Qu'est-ce que le phishing ?

Seq.4 : Repérer une tentative de phishing

Seq.5 : Différence http / https

Seq.6 : Identifier un lien malveillant

Seq.7 : Que faire face au phishing ?

Seq.8 : Politique du bureau propre

Seq.9 : Les risques liés aux clés USB

Seq.10 : Cybersécurité et télétravail

Seq.11 : Solliciter la DSI pour les logiciels

Seq.12 : Évaluation finale – Quiz

Seq.13 : Synthèse et fiche récapitulative

Outils

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

Date

- 1er novembre 2025