Formation prête à l'emploi

SÉCURITÉ INFORMATIQUE

NOTRE FORMATION EN LIGNE

Durée

✓ 20 min

Support

✓ Ordinateur
✓ Tablette
✓ Smartphone

Public concerné

✓ Tous les collaborateurs

Prérequis

✓ Aucun

Objectifs.

À l'issue de ce module les apprenants sauront :

- **Définir** les menaces en matière de détournement du système d'information
- **Reconnaître** les situations à risque
- **Agir** de façon appropriée pour assurer la protection des données

Démarche pédagogique.

- **Des activités pédagogiques** successives, insérées dans un scénario, portant sur des décisions à prendre ayant une incidence sur le niveau de sécurité des données
- **Une jauge** dont le niveau varie en fonction des choix faits : le niveau de cette jauge doit être supérieur ou égal à 80% pour valider le module
- **Des règles de sécurité/bonnes pratiques** sont découvertes au fil de la progression et sont toutes recensées à la fin du module

Modalités de déploiement.

- Module disponible en **location** sur notre plateforme **LMS**
  - *Licence annuelle par apprenant*

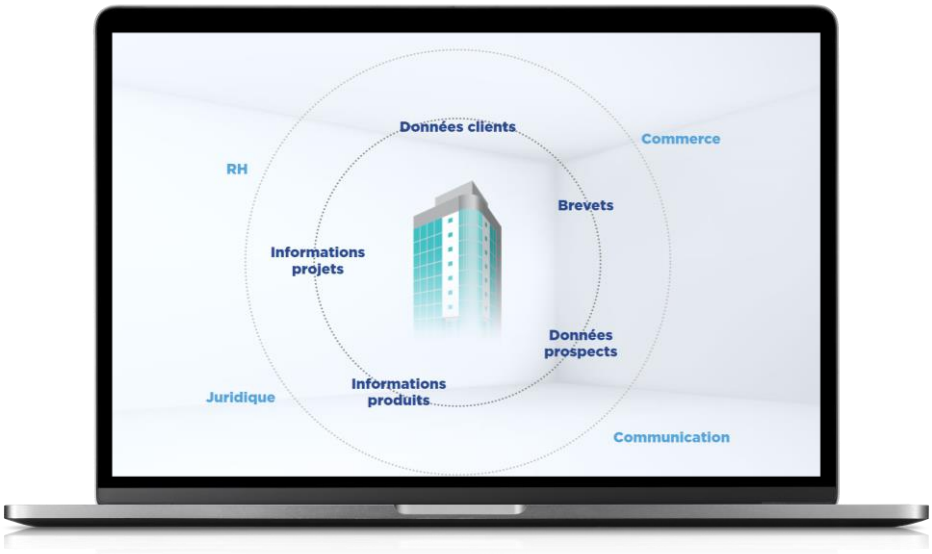
- Module disponible à **l'achat**
  - *Livraison du fichier SCORM, personnalisation du contenu possible*

SOMMAIRE DU MODULE

Partie 1 - Introduction.

La courte introduction explique que **la protection des informations sensibles est l'affaire de tous** : employés et partenaires de l'entreprise. Elle explicite ensuite les objectifs de la formation : donner les règles et bonnes pratiques à respecter pour pouvoir participer activement à la protection des données de son entreprise.

A cette fin **une séquence ludique est proposée** aux apprenant. Celle-ci est annoncée avec la présentation de la « règle du jeu » : des activités successives, contextualisées dans une journée, qui amèneront les apprenant à faire des choix qui auront une incidence sur le niveau de sécurité des données de l'entreprise, matérialisé par une jauge. La modalité de validation du module de formation est d'ores et déjà explicité avec un niveau de sécurité minimal à maintenir.



Partie 2 – En pratique.

Cœur du module, **cette seconde séquence plonge l'apprenant dans une journée de travail** et le confronte à de nombreuses situations à risques, sous forme d'activité pédagogique. Les bonnes pratiques à acquérir sont découvertes au fur et à mesure de la progression et l'explication de la menace est effectuée dans le feedback de chaque activité (thématiques abordées en page suivante).

Partie 2 (suite) – Thématiques abordées.

- **Mot de passe**
  - Mémoriser ses mots de passe et ne jamais les écrire où que ce soit
- **Echange avec le service informatique**
  - Communiquer sur les alertes et disfonctionnements détectés
  - Communiquer en cas de perte ou de vol
- **Gestion de la messagerie**
  - Vérifier l'adresse e-mail de l'expéditeur d'un e-mail avec d'ouvrir une pièce jointe
  - Reconnaître un e-mail frauduleux (tentative d'hameçonnage)
- **Appareils et sécurité**
  - Utiliser des périphériques/supports de stockage de confiance, uniquement ceux fournis par son entreprise
  - Maintenir la distinction entre appareils personnels et appareils professionnels
- **Software de protection**
  - Disposer d'un antivirus/antispam
- **Préservation** des données
  - Sauvegarder les données et utiliser les serveurs de son entreprise
  - Partager un fichier professionnel en externe en utilisant les outils adaptés
- **Déplacement et règles de sécurité à respecter**
  - Ne pas laisser son ordinateur accessible sans surveillance
  - Verrouiller son ordinateur lorsque l'on ne n'utilise pas
  - Utiliser une connexion réseau wifi sécurisée

Partie 3 – Conclusion.

Comme l'apprenant a pu le découvrir à travers les situations à risques, la conclusion insiste sur **le rôle essentiel joué par chaque collaborateur dans la protection des données** et sur l'importance d'appliquer les règles découvertes tout au long du module.

En fonction du score obtenu dans la partie 2, le module sera validé ou l'apprenant sera invité à le rejouer. **L'ensemble des bonnes pratiques découvertes au fur et à mesure sont accessibles dans un pop-up**.