Formation SSI : Sensibilisation à la cybersécurité pour les employés

PLUS D'INFOS

- Contactez-nous

CONTACT REFERENT

- Commercial@ageris-group.com
- +33 3 87 62 06 00

MODALITES D'ACCES

- Inscription en réservant votre place sur une session disponible ou par téléphone, par mail, par demande de contact. Vous recevrez un devis à nous retourner avec votre accord pour confirmer votre inscription.

DELAI D'ACCES

- La durée estimée entre la demande du stagiaire et le début de la formation est de 7 jours (peut être raccourci pour le mode distanciel)

ACCESSIBILITE AUX PERSONNES EN SITUATION D'HANDICAP

- Accessible à distance pour les personnes à mobilité réduite
- Pour connaître l'accessibilité aux salles de formation, vous pouvez nous joindre au +33 3 87 62 06 00

REFERENCE

- SSISENSIEMPLOYES

TARIF

- 890 € HT

DUREE DE LA FORMATION

- 1 jour – 7 heures

DATES DES SESSIONS

- Voir site internet

FINANCEMENT

- OPCO

FORMULE INTRA-ENTREPRISE

Formulaire : soumettez votre projet

RESSOURCES PEDAGOGIQUES

- Cours théorique
- Exemples concrets
- Evaluation des compétences par un quizz en cours et en fin de formation

PRESENTATION DE LA FORMATION

L'utilisation des ressources du système d'information n'est pas sans risque. Cette sensibilisation présente à l'aide de très nombreux exemples les bonnes pratiques de l'utilisateur sédentaire, nomade ou en télétravail pour limiter les risques d'erreur ou de malveillance.

OBJECTIFS DE CETTE FORMATION

- Connaître les bonnes pratiques pour limiter les risques juridiques et opérationnels.
- Savoir protéger les informations en adéquation avec les besoins métiers.

PUBLIC

Tous les salariés d'une entreprise.

PREREQUIS

Aucun prérequis n'est nécessaire.

PROGRAMME DETAILLE

1- Introduction

- Les préjugés à surmonter
- Les valeurs essentielles à protéger
- Les périmètres
- Les menaces

2- L'organisation et les responsabilités

- La direction générale
- Les directions métiers
- La DSI
- Les sous-traitants
- La voie fonctionnelle SSI et le RSSI
- La voie fonctionnelle protection de la vie privée et le DPO
- Les administrateurs techniques et fonctionnels
- Les utilisateurs

3- Les référentiels SSI et vie privée

- Les politiques
- Les chartes
- Les guides et manuels
- Les procédures

4- Vision synthétique des obligations légales

- Disciplinaire
- Contractuelle
- Civiles
- Pénales
- Le cas du contrôle par l'employeur
    - Utilisation professionnelle
    - Utilisation non professionnelle

5- Les menaces

- La divulgation d'information « spontanée »
- L'ingénierie sociale et l'incitation à dire ou faire
- Le lien avec l'intelligence économique
- Le lien avec l'espionnage industriel

6- Les risques

- Vol, destruction
- Virus
- Les aspirateurs à données

Formation SSI : Sensibilisation à la cybersécurité pour les employés

- Support de cours remis au stagiaire en fin de formation
- Outil distanciel : Teams

POUR ALLER PLUS LOIN

- SSI – Devenir Responsable de la Sécurité des Systèmes d'Information (RSSI)
- SSI – Maîtriser l'analyse des risques du système d'information

PLUS D'INFOS

- Contactez-nous

- Le phishing /l'hameçonnage
- Les malwares
- Les spywares
- L'usurpation
- L'usurpation
- Les virus
- Le cas des réseaux sociaux

7- Les bonnes pratiques d'évaluation de la sensibilité de l'information

- La classification par les impacts, (juridiques, opérationnels, financiers, image, sociaux)
- L'échelle d'impact
- Les pièges

8- Les bonnes pratiques pour les comportements généraux

- A l'intérieur des établissements
- A l'extérieur des établissements

9- Les bonnes pratiques d'utilisation des supports d'information sensible pour les phases de conception, stockage, échanges et fin de vie

- Papier
- Environnement partagé
- Environnement individuel sédentaire
- Environnement individuel mobile

10- Les bonnes pratiques d'utilisation des ressources du système d'information

- Installation et maintenance
  - Postes fixes
  - Equipements nomades
  - Portables
  - Ordiphones
- Identification et authentification
- Échanges et communications
  - Intranet
  - Internet
  - Contrôle des certificats serveurs
  - Les échanges de fichiers via la plateforme « institutionnelle »
  - Le nomadisme
  - Les télétravailleurs et le VPN de télé accès
  - Email
  - La consultation en Web mail
  - Signature
  - Chiffrement
  - Cloud
  - Réseaux sociaux et forums thématiques professionnels et privés
  - Téléphonie
- Stockages et sauvegardes, (clés usb, locales, serveurs, …)
- Archivages
- Anonymisation
- Destruction ou recyclage

11- Conclusion

- Les engagements de responsabilité

MODALITES D'EVALUATION

Validation des connaissances et compétences par un quizz à la fin de chaque chapitre.