Formation « KIMIC »
Kit Minimum de Cybersécurité

Réf : Form_001

MAJ 01/01/2022

https://intelfe.com
contact@intelfe.com

La formation KIMIC est dédiée à tout utilisateur d'internet et d'outils numériques pour apprendre à protéger ses données et celles de son entreprise.
L'objectif de la formation est de permettre à tout particulier et/ou professionnel, d'appréhender les bonnes pratiques de cybersécurité, grâce à l'acquisition de connaissances sur les cybermenaces et le minimum requis pour protéger sa vie numérique.
Pour l'entreprise, cela optimisera son niveau en matière de cybersécurité globale des utilisateurs et limitera considérablement ses risques de cyber incidents, ce qui participera à sa conformité au RGPD ou à l'ISO 27001.
Au-delà de la sensibilisation, l'approche de cette formation se veut opérationnelle et pragmatique avec la présentation d'outils simples et le plus souvent gratuits qui permettent de savoir comment mettre en œuvre ces bonnes pratiques.

Objectifs

- Connaitre les cybermenaces et les principales bonnes pratiques en matière de cybersécurité pour utilisateur
- Savoir gérer ses mots de passe et se créer une authentification multi facteurs pour ses comptes principaux
- Savoir chiffrer des documents pour les stocker ou les transmettre de manière à garantir la confidentialité
- Savoir réaliser une sauvegarde automatisée de ses documents et comprendre les principes de mise à jour
- Savoir reconnaître les attaques par ingénierie sociale pour limiter les cyber incidents

Public visé

- Tout utilisateur d'un ordinateur (PC ou MAC), utilisateur d'internet
- Tout dirigeant, RH, manager,
- Tout personnel comptable, logistique, commercial, administratif…
- Toute personne qui traite des données sans avoir été formée à les protéger.

Prérequis

- Aucun prérequis n'est demandé cependant avoir de bonnes bases sur l'utilisation d'un ordinateur et d'internet (navigation, téléchargement, installation…) est un vrai plus
- Se munir d'un ordinateur avec Windows de préférence ou MAC

Durée & horaires

- 1 journée, soit 7 heures
- Horaires en présentiel : de 09h00 à 12h30 et de 14h à 17h30
- Horaires en distanciel : sur 2 demi-journées (soit matin, soit après midi)

Modalités de participation et d'accès

- Minimum 4 participants – Maximum 10 participants
- Lieu de formation choisi selon les besoins et la disponibilité des salles de formation
- Entretien préalable pour prendre en considération les situations de handicap afin de mettre en œuvre les adaptations pédagogiques, organisationnelles, matérielles ou autres, dans la mesure du possible.

Certification

- Cette formation n'est pas certifiante, au sens de France Compétences.

Méthode et moyens pédagogiques

- Formation réalisée en présentiel ou distanciel selon la formule retenue
- Formation construite avec une pédagogie basée sur l'analogie avec l'usage de la voiture
- Focus sur les points clés de la cybersécurité pour l'utilisateur
- Des cas pratiques pour savoir comment utiliser certains outils
- Espace collaboratif le temps de la formation et espace communautaire après la formation

Supports

- Support de cours au format pdf, en français
- Kit d'outils et ressources fournis pendant et après la formation
- Feuille d'émargement par demi-journée et délivrance d'un certificat de réalisation de la formation

Modalité d'évaluation de la formation

- Cas pratique pendant la formation et QCM en fin de formation
- Formulaire d'évaluation à chaud remis aux stagiaires à l'issue de la formation, afin de recueillir leurs impressions et identifier les axes d'amélioration éventuels

Programme

1. **Présentation**
2. **Connaître les cybermenaces**
   a. Exemples de cyber attaques
   b. Cybersécurité et principe d'une attaque
   c. Environnement numérique
3. **Gérer et sécuriser ses accès**
   a. Fiabilité d'un mot de passe
   b. Gestionnaire de mots de passe
   c. Authentification multi facteurs
4. **Comprendre la notion de vulnérabilité et l'importance des mises à jour**
   a. Les vulnérabilités
   b. Les sources à connaître et à suivre
   c. Les mises à jour (OS, navigateurs…)
5. **Sécuriser ses données sensibles**
   a. Principe du chiffrement
   b. Transmettre des données sensibles
   c. Stocker des données sensibles
6. **Sauvegarder ses données**
   a. 10 Points clés
   b. Stratégie de sauvegarde (3.2.1)
   c. Automatiser sa sauvegarde
7. **Reconnaitre une attaque ou une fraude par ingénierie sociale**
   a. L'ingénierie sociale
   b. Détection de phishing
   c. Détection de fraudes
8. **Que faire en cas d'incident**

Tarifs, délai d'accès et contact

- Formation inter entreprise : 690 € HT / Personne
- Formation intra entreprise : nous contacter
- Capacité de mise en œuvre de la formation dans les 2 mois en présentiel, dans le mois en distanciel
- S'inscrire au minimum 15 jours avant une date de formation précisée sur notre site

- Contact :

contact@intelfe.com
07.81.03.09.46
www.intelfe.com
Frédéric Lenfant

https://lstu.fr/kimic-by-intelfe