Programme de Formation

Initiation à la Sécurité des Systèmes d'Information

Organisation

Début : **Fin :** **Durée :** 7 heures

Mode d'organisation : Présentiel

Contenu pédagogique

Public visé

- Salariés, indépendants, agents publics
- Professionnels utilisant un ordinateur, un smartphone ou Internet dans leur activité
- Collaborateurs non informaticiens souhaitant adopter de bonnes pratiques numériques

Objectifs pédagogiques

À l'issue de la formation, les participants seront capables de :

- Comprendre les enjeux de la sécurité des systèmes d'information
- Identifier les principales menaces numériques
- Adopter des comportements numériques sûrs au travail et à domicile
- Sécuriser leurs outils de communication et de travail (PC, smartphone, objets connectés)
- Prévenir les attaques courantes telles que le phishing, les rançongiciels ou les virus

Description

1. Introduction à la SSI

- Définition de la sécurité des systèmes d'information (SSI)
- Rôle et missions des organismes de SSI en France (ANSSI, CNIL…)
- Enjeux européens : RGPD et cybersécurité

2. Sécurité des courriels

- Identifier les menaces : SPAM, SCAM, phishing (hameçonnage), rançongiciels
- Apprendre à vérifier la véracité d'un e-mail
  - Analyse des liens suspects
  - Précautions avec les pièces jointes

3. Sécuriser son poste de travail

- Comprendre les rôles des antivirus, antimalwares, pare-feux
- Tenir ses logiciels à jour
- Sauvegarder ses données efficacement (automatisée ou manuelle)

4. Navigation Internet sécurisée

- Le protocole HTTPS et son importance
- Comprendre le fonctionnement des cookies et des scripts
- Sécuriser son navigateur web (extensions, réglages, alertes de sécurité)
- Mots de passe : bonnes pratiques, gestionnaires de mots de passe, double authentification

5. Sécurité des appareils mobiles

- Sécuriser son smartphone ou sa tablette (Android et iOS)
  - Paramétrage du Wi-Fi, GPS, Bluetooth, NFC
  - Choisir les bonnes applications et limiter les autorisations
  - Utilité des antivirus mobiles
- Verrouillage d'écran et géolocalisation en cas de perte

6. Objets connectés (IoT) : menaces et précautions

- Identifier les risques liés aux objets connectés (caméras, assistants vocaux, montres…)
- Comprendre leurs vulnérabilités (mots de passe faibles, absence de mises à jour)
- Bonnes pratiques pour sécuriser ces équipements

Prérequis

Connaissances et manipulations de base en informatique (fonctionnement d'un ordinateur, utilisation courante)

Modalités pédagogiques

ateliers pratiques et exercices de mise en application

Moyens et supports pédagogiques

Un ordinateur par stagiaire, un support de cours

Modalités d'évaluation et de suivi

Évaluation en fin de formation par un questionnaire à choix multiples

Informations sur l'admission

Informations sur la formation en présentielle

- **Lieu** : les stagiaires suivront la formation dans nos locaux (2 avenue Leonard de Vinci, 63000 Clermont- Ferrand
- **Horaires** : 9h -12 h 30// 13h 30- 17 h avec pauses.
- **Interactivité** : échanges directs avec le formateur, travaux pratiques, questions-réponses.
- **Supports** : documents papier ou numériques remis aux participants.
- **Matériel** : chaque stagiaire dispose d'un poste informatique.

Informations sur l'accessibilité

Etablissement ERP
Accessibilité aux personnes en situation de Handicap