

Formation Sécurité informatique

Durée formation

4 jours

Objectifs

Sensibiliser les professionnels à la sécurité informatique. Comprendre le fonctionnement de Windows, savoir le sécuriser. Connaître les types d'agressions possibles et s'en prémunir.

Publics concernés

TPE, professions libérales soucieuses de se familiariser aux bases de la sécurité informatique. Avoir des connaissances sur le fonctionnement des réseaux est recommandé.

Contenu de la formation

Windows

- Sécuriser Windows
- Auditer des objets ou des évènements
- Intérêt de l'outil Windows Update
- Connaître les processus et les services lancés au démarrage
- Utilisation du gestionnaire des tâches
- Les différents services Windows
- Créer un mot de passe solide
- Définir des stratégies pour les mots de passe
- Désactiver les partages administratifs
- Les droits et les autorisations NTFS
- Savoir définir des autorisations personnalisées sur les partages

Anonymat

- Effacer les traces de sa navigation sur Internet
- Supprimer les MRU (fichiers récemment utilisés)
- Supprimer définitivement des fichiers ou des dossiers

Réseau

- Vérification des ports ouverts sur une machine
- Fermer les ports inutiles
- Le fichier HOST

Applications

- Sécuriser Internet Explorer
- Utiliser HijackThis
- Gestion des pièces jointes
- Sécuriser Outlook et Outlook Express
- Installation de logiciels pour sécuriser les processus et les données sensibles

Sécurité

- Utilité d'un antivirus
- Mise à jour de l'antivirus – Scan régulier du système
- Installation et fonctionnement d'un firewall
- Analyse Firewall (leaktest, test de vulnérabilité)
- Connaître les différents ennemis (rootkits, virus, ver, trojan, spyware, keylogger, adware) et comment s'en prémunir

Divers

- Qu'est-ce que le Social Engineering ?
- Quelques règles de bonnes conduites pour éviter les problèmes en informatique