Bonnes pratiques pour défendre son système informatique des menaces en ligne et sur site - 2 jours

Informatique

Fondamentaux, règlementation et Synthèses

Référence : 4-SE-DEF
Durée : 2 jours
Présentiel ou en classe à distance

Tarif Inter : 750 € Prix HT jour / personne
Tarif Intra : 1500 € Prix HT jour / groupe

Mise à jour : 27/11/2023

Durée de validité : du 01/01/2026 au 31/12/2026

Objectifs

Aider les responsables des TPE et PME à protéger leur entreprise des menaces informatiques

Prérequis

Une réelle connaissance informatique est nécessaire

Public concerné

Responsable de services informatiques et intervenants techniques (service IT)

Contenu pédagogique

Accueil et introduction

- Présentation de l'objectif du cours
- Brève introduction à la cybersécurité

Les menaces en ligne pour les TPE et PME

- Les principales menaces en ligne : phishing, ransomware, malware, etc.
- Les menaces venant de l'intérieur : virus, vol de données, destruction de données...
- Exemples de cas réels de cyberattaques contre les petites entreprises
- Les conséquences financières et de réputation des cyberattaques

Bonnes pratiques et cybersécurité

- Utilisation de mots de passe forts et uniques
- Cryptage de fichiers
- Mises à jour régulières des logiciels
- Sensibilisation à l'email et aux pièces jointes suspectes
- Sensibilisation aux bonnes pratiques : usb, échanges de documents, gestion des comptes...
- Travail à distance et prestataires extérieurs
- Accès au réseau en inter, Wi-Fi...

Comment sécuriser mon environnement

- Le poste de travail
- Outils et conseils pour sécuriser le poste utilisateur (Windows 10/11...)

Suite de la sécurisation du poste client

- Rappels des technologies disponibles dans Windows : Antivirus, boot sécurisé...
- Sécurisation par GPO
- Cryptage de postes et des fichiers
- Gestion des certificats

Comment sécuriser le domaine et Active Directory ?

- Comment bien organiser Active Directory et les GPO
- Renforcer la gestion des comptes et des groupes pour éviter les failles

Comment surveiller Active Directory ?

- Comment surveiller son SI à la recherche d'anomalies
- Bonnes pratiques et sources d'informations pour aller plus loin...

Comment sécuriser mon serveur de fichiers ?

- Bonnes pratiques pour gérer le serveur et les permissions sur les fichiers
- Outils pour sécuriser le serveur de fichiers
- Gestionnaire de ressources, sysinternals...
- Comment surveiller les accès aux fichiers ?

Sécuriser les services réseaux du quotidien

- Service DHCP et serveur DNS : quels risques et quelles solutions ?
- Gestion des accès depuis l'extérieur : VPN, Web, Rds...
- Gestion du Wifi : accès privé / accès public

Gestion des mises à jour serveurs et postes clients

- Mise à jour manuelle ou automatisée
- Mise à jour des postes clients : obligatoire / falcultative
- Mise à jour des serveurs : bonnes pratiques ?

Serveurs d'impressions et serveurs applicatifs

- Comment augmenter la sécurité de l'impression
- Bonnes pratiques pour les serveurs applicatifs

Prévoir un plan de reprise et de continuité en cas d'attaques ou de panne

- Évaluer les risques
- Définir les priorités
- Assurer la continuité

Moyens pédagogiques

- Réflexion de groupe et apports théoriques du formateur.
- Travail d'échange avec les apprenants sous forme de réunion - discussion.
- Utilisation de cas concrets issus de l'expérience professionnelle.
- Validation des acquis par des questionnaires, des tests d'évaluation, des mises en situation et des jeux pédagogiques.
- Alternance entre apports théoriques et exercices pratiques (en moyenne sur 30 à 50% du temps)

Modalités pédagogiques : Présentiel, Distanciel et AFEST

Moyens techniques

En formation présentielle

Accueil des apprenants dans une salle dédiée à la formation et équipée avec :

- Ordinateurs
- Vidéo projecteur ou Écran TV interactif
- Tableau blanc ou Paper-Board

En formation distancielle

A l'aide d'un logiciel comme ® Microsoft Teams ou Zoom, un micro et une caméra pour l'apprenant.

- Suivez une formation en temps réel et entièrement à distance. Lors de la session en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur.
- Les formations en distanciel sont organisées en Inter-Entreprise comme en Intra-Entreprise.
- L'accès à l'environnement d'apprentissage (support de cours, ressources formateur, fichiers d'exercices ...) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré.
- Les participants recevront une convocation avec le lien de connexion à la session de formation.
- Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition par téléphone au 02 35 12 25 55 ou par email à commercial@xxlformation.com

Modalités d'évaluation

- Positionnement préalable oral ou écrit.
- Feuille de présence signée en demi-journée.

- Evaluation des acquis tout au long de la formation.
- Questionnaire de satisfaction
- Attestation de stage à chaque apprenant
- Evaluation formative tout au long de la formation.
- Evaluation sommative faite par le formateur.

Profil du formateur

- Nos formateurs sont des experts dans leurs domaines d'intervention
- Leur expérience de terrain et leurs qualités pédagogiques constituent un gage de qualité

Adaptation pédagogique et matérielle

Si vous avez besoin d'adaptation matérielle ou pédagogique, merci de prendre contact avec notre référent Handicap par téléphone au 02 35 12 25 55 ou par email à handicap@xxlformation.com

Modalités et délais d'accès à la formation

Les formations sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.

Nos sessions INTER 2026

Sessions de formation à venir :

- Aucune session à venir pour cette formation.

Nos sessions INTRA 2026

Pour organiser cette formation en intra-entreprise, veuillez nous contacter par mail à commercial@xxlformation.com ou par téléphone au 02 35 12 25 55