A.C.F

SECURITE VULGARISATION RESEAU

Public	Personnels non techniques travaillant dans un environnement IT Assistants, administratifs, fonctions support, chefs de projets débutants Étudiants ou professionnels souhaitant une première approche de la cybersécurité réseau
Durée	1 journée - 7 heures
Pré-requis	Aucune connaissance technique particulière. Être à l'aise avec l'utilisation générale d'un ordinateur et d'internet.
Objectifs	Comprendre les bases d'un réseau informatique Appréhender les principes fondamentaux de la cybersécurité réseau Identifier les risques courants en entreprise liés à la sécurité informatique Analyser des situations concrètes et adopter des bonnes pratiques
Méthodes pédagogiques	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
Moyens techniques	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
Modalité d'évaluation des acquis	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
Délai d'accès	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
Accessibilité handicapés	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

MATINÉE (3H30)

1. INTRODUCTION GÉNÉRALE

- Pourquoi parler de réseau et de sécurité aujourd'hui ?
- Risques quotidiens en entreprise
- Vue d'ensemble d'un réseau informatique

2. LES BASES DU RÉSEAU (AVEC SCHÉMAS SIMPLES)

- Qu'est-ce qu'un réseau local (LAN) ?
- Routeur, switch, câbles, Wi-Fi : les rôles de chacun
- Introduction aux adresses IP (sans complexité)
- Différence entre Internet, Intranet et Extranet
- Activité ludique : mini-jeu "Dessinez votre réseau de bureau"

3. LES CONCEPTS RÉSEAU APPLIQUÉS À LA SÉCURITÉ

- Qu'est-ce qu'un VLAN ? (métaphore : bureaux fermés dans un open space)
- Qu'est-ce qu'une DMZ ? (zone tampon entre l'entreprise et Internet)
- Qu'est-ce qu'un firewall ? (comparaison avec un filtre ou un videur)

4. CAS PRATIQUES ILLUSTRÉS

- Exemple d'une entreprise sans VLAN ni firewall problèmes
- Mise en place d'un VLAN pour séparer l'administration du reste
- Utilité d'une DMZ pour un site web public

APRÈS-MIDI (3H30)

1. TERMINOLOGIE DE LA SÉCURITÉ INFORMATIQUE

- Définitions simples : malware, phishing, antivirus, pare-feu, VPN, MFA
- Rôle des mots de passe, des mises à jour, et des sauvegardes
- Notion de "surface d'attaque" et de "principe du moindre privilège"

2. APPLICATION CONCRÈTE À L'ENTREPRISE

- Cas d'usage : Réseau d'une TPE/PME typique, risques liés au Wi-Fi invité, exposition d'un serveur web
- Bonnes pratiques en entreprise : ne pas brancher n'importe quoi, vigilance sur les mails, demander l'avis de l'IT

3. ATELIER PRATIQUE

- Lecture commentée d'un schéma réseau simplifié
- Identification des zones sensibles

4. SYNTHÈSE, ÉCHANGES, ET MISES EN SITUATION

- Jeu de rôle : "Vous êtes responsable de la sécurité d'un petit bureau"
- Discussion ouverte : "Que pouvez-vous améliorer dans votre entreprise ?"
- Q/R – Debriefing

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Téléphone
04 76 23 20 50 - 06 81 73 19 35

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !

ACF Audit Conseil Formation

@ACF_Formation

Dernière mise à jour : 24/07/2025