

NAVIGATION WEB SENSIBILISATION À LA SÉCURITÉ

— Public	Tout public ayant une utilisation de la navigation web et des services d'e-mail.
— Durée	1 journée - 7 heures
— Pré-requis	Aucune connaissance particulière.
— Objectifs	Appréhender les menaces et concepts de sécurité autour de l'utilisation du web Utiliser Internet en étant conscient des risques Naviguer avec un niveau de sécurité satisfaisant Contrôler la diffusion de ses informations personnelles Acquérir les bonnes pratiques de sécurité pour la navigation web
— 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.

LES PRINCIPALES MENACES RENCONTRÉES SUR LE WEB

- Bulle de filtrage et ciblage publicitaire.
- Fake news et canular (hoax).
- Le phishing (hameçonnage) : e-mails et sites frauduleux.
- Les pièces jointes à un courriel.
- Piratage de compte et d'identité.

DONNÉES PERSONNELLES ET BONNES PRATIQUES DE NAVIGATION

- Le contrôle de la diffusion des données personnelles sur le web.
- Gestion des mots de passe et moyens d'authentification.
- Bloqueurs de pubs et de sites malveillants.
- Mise à jour des logiciels et désactivation de composants.
- La sauvegarde régulière de ses données.
- Les réglementations française, européenne et nord-américaine relatives à la protection des données.
- Signalement des pratiques frauduleuses.

LES MÉCANISMES DE CONFIANCE POUR LE WEB

- HTTPS : le web sécurisé.
- Focus sur les clés de chiffrement : cryptage, hachage et vérification d'intégrité.
- Les certificats SSL/TLS : présentation et typologie.
- Organismes de certification et certificats auto-signés.
- Le paiement en ligne.

APPROCHE TECHNIQUE DES ATTAQUES SUR LE WEB

- Typologie des pirates et leurs objectifs.
- Doxxing, hot-reading, stalking.
- Malware : les pièces jointes infectées dans les e-mails.
- Le cas particulier des ransomwares (rançongiciels).
- JavaScript : clickjacking, cross-site scripting (XSS) et CSRF.
- Les types d'attaques directes et par rebond.
- Man in the middle.
- Dénî de service et DDoS.

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 : 12/12/2024

PROFIL Formateur : Les formateurs sont recrutés selon plusieurs critères :
Expérience, pédagogie, dynamisme et prévoyance.