INITIATION DE L'UTILISATEUR À LA CYBERSÉCURITÉ

Public	Toute personne utilisant du matériel informatique professionnel ou personnel.
Durée	3,5 heures jours - 25 heures
Pré-requis	Accessible à tout le monde
Objectifs	Comprendre ce qu'est-ce que la Cybersécurité Comprendre les enjeux de la cybersécurité en entreprise, individuel gouvernemental Comprendre pourquoi on nous menace Les principes fondamentaux de la cybersécurité Notion sur les différentes attaques Maitriser les Points de vigilances Comprendre les failles des logiciels Acquérir les bonnes pratiques pour une meilleure sécurité. Conseils pour les déplacements pro/perso Comment réagir face à une cyberattaque en entreprise
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.

QU'EST-CE QUE LA CYBERSÉCURITÉ

- Pour les individus, pour les entreprises, pour les gouvernements et infrastructures critiques
- Pourquoi est-ce Important ?
- Les principes fondamentaux de la cybersécurité (Confidentialité, Intégrité, Disponibilité)

QUI ME MENACE

- Photo-expression : exprimez-vous : connaitre le profil des cyberattaquants
- Sa représentation du cyberattaquant en photo, exprimer les émotions
- Définitions : Cybercriminels, Hacktivistes, Etats-Nations, Employés Mécontents, Script Kiddies

QUELLES SONT LES PRINCIPALES ATTAQUES :

- Quel nom d'attaque vous vient à l'esprit lorsqu'on parle de cyberattaque ?
- Les menaces courantes en cybersécurité
- Déf : Malwares, Virus, Ransomware Spyware, Adware
- Explications attaques DDoS, Ingénierie sociale (attaque RIB, attaque au président…)
- Ce qu'il faut retenir des attaques d'ingénierie sociale : Comment se protéger de l'ingénierie sociale : reflexes individuels
- Attaque de l'Homme du Milieu : explications
- Vulnérabilité des Logiciels
- Les 10 attaques les plus courantes et comment elles vous Manipulent : principe de l'attaque, pourquoi ça marche, Exemples.

LES BONNES PRATIQUES POUR UNE MEILLEURE SÉCURITÉ

- Les Mots de passe : explications longueurs et recommandations ANSSI.
- Gestionnaire de mot de passe
- Les adresses Mails : les points de vigilance…. Nom de l'expéditeur, les liens, les pièces jointes, les fautes d'orthographe, informations contenues dans le mail. Exemples d'arnaque par mail.
- Explication MFA, mise à jour, sauvegardes, pare-feu, antivirus, anti-spam.
- Exemple de fichiers Cryptés

CONSEILS AUX VOYAGEURS

- Recommandations de l'ANSSI aux voyageurs en déplacement en France ou à l'étranger avec son téléphone, sa tablette ou son ordinateur portable.
- Point sur les wifi des cybercafés, hôtels, lieux publics.
- Conseils Avant de partir : les filtres de protection des écrans, signes distinctifs des appareils.
- Pendant la mission :
- En cas de perte ou vol des équipements
- Mot sur les points de recharges électrique en libre-service.
- Au retour de mission

QUELS POINTS DE VIGILANCES

- Mur collaboratif faire identifier sur un mur collaboratif les points de vigilances en rapport ; aux Mails, site web, sms, Autres…

COMMENT RENFORCER SA CYBERSÉCURITÉ

- Effet boule de neige
- 3 Questions : Quelles sont les bonnes pratiques pour renforcer ma sécurité numérique ?
- Comment protéger les données sensibles en entreprise ?
- Comment réagir face à une cyberattaque en entreprise ?
- Temps 1 : seul, Temps 2 par 2, temps 3 par 4, mises en commun rapporteur.

DISTRIBUTION DE DOCUMENTS

- Consignes en cas de cyberattaque.

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 : 18/11/2025

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