

INITIATION DE L'UTILISATEUR A LA CYBERSECURITE

Public	Toute personne utilisant un ordinateur, un smartphone ou Internet dans un cadre personnel ou professionnel.
Durée	½ journée - 4 heures
Pré-requis	Aucun
Objectifs	Comprendre les enjeux de la cybersécurité et identifier les principaux risques liés aux usages numériques Reconnaître les principales cybermenaces (virus, ransomware, phishing, etc.) et leurs modes de fonctionnement Détecter les tentatives de fraude, notamment les attaques de phishing et d'ingénierie sociale Adopter les bonnes pratiques de sécurité au quotidien et réagir efficacement en cas d'incident
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)

INTRODUCTION À LA CYBERSÉCURITÉ

- Définition de la cybersécurité
- Pourquoi la cybersécurité est importante pour les particuliers et les entreprises
- Les principes fondamentaux de la cybersécurité : confidentialité, intégrité, disponibilité

COMPRENDRE LES CYBERMENACES

- Les différents profils de cyberattaquants
- Les motivations des cyberattaques
- Les menaces les plus courantes : virus, ransomware, spyware et adware
- Les attaques par déni de service (DDoS)
- L'exploitation des vulnérabilités logicielles
- Les fuites et vols de données

PHISHING ET INGÉNIERIE SOCIALE

- Définition du phishing et de l'ingénierie sociale
- Les techniques de manipulation utilisées par les cybercriminels
- Les formes courantes d'attaques : faux emails, fraude au président, fraude au RIB, faux SMS
- Les signes permettant d'identifier un message frauduleux
- Analyse d'exemples concrets de tentatives de phishing

LES BONNES PRATIQUES DE CYBERSÉCURITÉ

- Les règles essentielles pour sécuriser ses usages numériques
- Bonnes pratiques pour les mots de passe
- Utilisation de l'authentification multi-facteurs (MFA)
- Vigilance face aux emails, liens et pièces jointes
- Importance des mises à jour et des outils de protection (antivirus, anti-spam, pare-feu)

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 VIGILANCE

- Mur collaboratif faire identifier sur un mur collaboratif les points de vigilance 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

RÉAGIR FACE À UNE CYBERATTAQUE

- Reconnaître les signes d'une attaque ou d'un comportement suspect
- Les bons réflexes en cas d'incident de sécurité
- Procédure de signalement en cas de cyberattaque

CONCLUSION

- Récapitulatif des bonnes pratiques
- Ressources utiles (ANSSI, CNIL)
- Questions / réponses

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 : 20/03/2026

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