

— Public	Tout public
— Durée	½ journée - 4 heures
— Pré-requis	Aucun
— Objectifs	Identifier les principales menaces cyber et comprendre leurs mécanismes. Appliquer les bonnes pratiques de cybersécurité au quotidien, tant en usage personnel que professionnel. Reconnaître et réagir face à une tentative de phishing, ransomware ou compromission de compte. Comprendre les enjeux de sécurité liés à l'administration des systèmes d'information.
— 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.

INTRODUCTION À LA CYBERSÉCURITÉ (30 MIN)

1. DÉFINITION ET CONTEXTE

- Pourquoi la cybersécurité est-elle cruciale aujourd'hui ?

2. LES PRINCIPALES CYBERMENACES :

- Malware (virus, ransomware, spyware)
- Attaques par déni de service (DDoS)
- Exploitation de vulnérabilités logicielles
- Fuites de données et violations de la vie privée

3. EXEMPLES CONCRETS

- Etudes de cas récentes (entreprises, administrations, particuliers)

4. RÔLE DE CHACUN

- Comment contribuer à la sécurité de son organisation ou de ses données personnelles ?

SÉCURITÉ DES SYSTÈMES ET DES RÉSEAUX (45 MIN)

1. SÉCURITÉ DES POSTES DE TRAVAIL

- Mises à jour régulières (OS, logiciels, antivirus)
- Utilisation de pare-feu et d'outils de détection (EDR, antivirus)
- Gestion des droits d'accès (principe du moindre privilège)

2. SÉCURITÉ DES RÉSEAUX

- Wi-Fi sécurisé (WPA3, VPN)
- Risques des réseaux publics
- Segmentation du réseau

3. ATELIER PRATIQUE

- Vérification des paramètres de sécurité sur un poste (Windows/Mac/Linux)

SÉCURITÉ DES DONNÉES ET PROTECTION DE LA VIE PRIVÉE (45 MIN)

1. CHIFFREMENT

- Pourquoi et comment chiffrer ses données (disques, emails, messagerie)

2. SAUVEGARDES

- Stratégie 3-2-1 (3 copies, 2 supports différents, 1 hors site)

3. PROTECTION DES DONNÉES SENSIBLES

- RGPD et bonnes pratiques
- Gestion des mots de passe (gestionnaires, 2FA)
- Partage sécurisé de fichiers

4. ATELIER PRATIQUE

- Création d'un coffre-fort numérique ou configuration d'un gestionnaire de mots de passe

RÉAGIR FACE À UNE CYBERATTAQUE (30 MIN)

1. SIGNES D'UNE INTRUSION OU D'UNE ATTAQUE

- Comportement anormal du système
- Activité réseau suspecte
- Messages d'alerte ou demandes inhabituelles

2. PROCÉDURES D'URGENCE

- Isolation du poste ou du réseau
- Signalement à l'équipe IT ou au responsable sécurité
- Ne pas payer en cas de ransomware

3. CAS PRATIQUE

- Simulation d'une alerte et discussion sur les actions à mener

CONCLUSION ET RESSOURCES (15 MIN)

1. RÉCAPITULATIF DES BONNES PRATIQUES

2. RESSOURCES UTILES

- Sites de référence (ANSSI, CERT, CNIL)
- Outils gratuits (antivirus, gestionnaires de mots de passe, tests de sécurité)
- Formations en ligne (MOOC, webinaires)

3. 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 : 05/03/2026

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