



SENSIBILISATION UTILISATEURS AUX CYBERMENACES

— Public	Toute personne désirant se mettre à jour sur les nouveaux types de menaces informatiques.
— Durée	½ journée - 4 heures
— Pré-requis	Pas de pré-requis
— Objectifs	Sensibiliser les utilisateurs aux nouvelles menaces informatiques
— Méthodes pédagogiques	<p>Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire.</p> <p>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.</p> <p>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.</p>
— Moyens techniques	<p>1 poste de travail complet par personne</p> <p>De nombreux exercices d'application</p> <p>Mise en place d'ateliers pratiques</p> <p>Remise d'un support de cours</p> <p>Passage de certification(s) dans le cadre du CPF</p> <p>Remise d'une attestation de stage</p>
— Modalité d'évaluation des acquis	<p>Evaluation des besoins et objectifs en pré et post formation</p> <p>Evaluation technique des connaissances en pré et post formation</p> <p>Evaluation générale du stage</p>
— 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.

REPRENDRE LE CONTRÔLE SUR SA VIE PRIVÉE

- Prenez le temps de régler les paramètres de confidentialité
- N'en dites pas trop !
- Ne mélangez pas vie privée et vie professionnelle
- Ne publiez pas en temps réel
- Contrôlez le comportement des objets connectés
- Séparez les usages d'Internet à titre privé et professionnel
- Ayez une utilisation responsable des réseaux sociaux
- Maîtrisez votre communication sur les réseaux sociaux
- Vérifiez les sources avant de diffuser une information

BIEN GÉRER SES MOTS DE PASSE

- Utilisez des mots de passe différents pour le professionnel et le personnel
- Utilisez un mot de passe différent pour les services critiques
- Ayez un mot de passe robuste pour votre messagerie
- Ayez un mot de passe complexe (10 caractères minimum de type passphrase)
- Activez l'authentification forte sur les services critiques
- Verrouillez votre ordinateur
- N'écrivez pas un mot de passe
- Utilisez un gestionnaire de mot de passe
- Changez vos mots de passe à votre rythme

DES MISES À JOUR ET UN ANTIVIRUS POUR MIEUX VOUS PROTÉGER

- Redémarrez votre ordinateur pour valider les mises à jour
- N'attendez pas la fin de la journée pour redémarrer votre ordinateur
- Adoptez les mêmes règles pour vos équipements personnels
- En cas de longue absence, laissez le temps à votre antivirus de se mettre à jour avant d'ouvrir des e-mails
- Remettez-vous en question ! L'ordinateur vous fait confiance
- Gardez à l'esprit qu'un antivirus n'est efficace que contre ce qu'il connaît

ADOPTER LE BON COMPORTEMENT EN DÉPLACEMENT

- Sauvegardez vos données
- Ne voyagez pas avec votre support de sauvegarde
- Ne posez pas votre smartphone sur le coin d'une table, rangez-le !
- Gardez un œil sur vos équipements ou attachez-les. Conservez l'ordinateur avec les bagages à main, et non en soute.
- N'abordez pas de discussions sensibles dans des lieux publics.
- Utilisez des filtres de confidentialité sur vos écrans.
- A votre retour de voyage, changez vos mots de passe.
- A l'étranger, voyagez avec un ordinateur blanc. Ou avant de partir, supprimez du disque dur toutes les données confidentielles ou sensibles.
- Ne dites pas publiquement que vous êtes absent.

CONSIDÉRER SON SMARTPHONE COMME UN COFFRE-FORT

- Activez une authentification robuste (code pin 8 caractères ou empreinte digitale)
- N'affaiblissez pas les réglages de sécurité du système.
- Faites les mises à jour de sécurité sur système et applications
- Contrôlez les autorisations de vos applications
- Évitez les réseaux Wi-Fi publics ou inconnus
- Activez le chiffrement de l'appareil
- Utilisez une solution contre les malwares
- Sauvegardez vos données critiques
- N'installez que des applications issues du magasin officiel.

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 : 01/03/2021