

Sensibilisation à la cybersécurité

Formacode	31045
Public	Dirigeants et salariés
Prérequis	Aucun
DISPOSITIONS PRATIQUES	Effectif maximum : 8 participants
Modalités et délai d'accès	Inscription via notre bulletin d'inscription : au minimum 15 jours avant le démarrage de la session
Objectif	Protéger l'entreprise et ses salariés des menaces cyber
Contenu de la formation	Programme détaillé : <u>Les enjeux de la cybersécurité</u> 1.1. État de la menace 1.2. Risques pour l'entreprise 1.3. Législation / RGPD 1.4. Cas concret de cyberattaque <u>Identifier les menaces</u> 2.1. Sources de menaces 2.2. Failles et exploitations <u>Hygiène informatique (adopter les bonnes pratiques)</u> 3.1. Authentification / mots de passe 3.2. Messagerie 3.3. Mobilité / télétravail 3.4. Vie privée / vie personnelle (séparation des usages) 3.5. Poste de travail 3.6. Données sensibles <u>Que faire en cas d'attaques</u> 4.1. Premiers réflexes 4.2. Rendre compte 4.3. Conservations des preuves <u>Synthèse finale</u>
Modalités pédagogiques	Moyens pédagogiques : • Matériel informatique : Ordinateur, écran ou vidéo projecteur • Salles ;

SIEGE :

UNITÉ INFORMATIQUE - ROCADE SUD
480 Rue des tisserands
40280 SAINT-PIERRE-DU-MONT

SIRET 329 814 321 00025 RCS MONT DE MARSAN - APE 6202B

☎ 05.58.06.23.23

BASES TECHNIQUES :

• AQUITAINE
Mini-Parc Bât 3 - Rue du Pr A. Lavignolle, 33300 BORDEAUX
☎ 05.56.11.20.90 - SIRET 329 814 321 00041

• NORMANDIE - CAEN
3 rue Martin-Luther King, 14280 Saint-Contest
☎ 02.31.44.36.87 - SIRET 329 814 321 00066



	Jeu interactif Matériel de démonstration Méthodes : • Active, • Interrogative • Magistrale • Démonstrative • Collaborative Modalités : Présentiel, à distance, mode projet, autoformation accompagnée, ... Point en amont de la formation avec restitution du besoin client. Point en fin de journée de formation, recueil des impressions, régulation sur les autres journées en fonction de l'évolution pédagogique. Évaluation à chaud en fin de formation, débriefing sur l'écart éventuel, formalisation d'une régulation sur les points soulevés.
Moyens d'encadrement de la formation	IMPI s'engage à adapter chaque formation aux besoins réels du stagiaire. L'animation est basée sur une pédagogie active, avec des exercices pratiques et personnalisés qui permet l'ancrage en temps réel. Cette animation s'appuie sur une alternance d'exposés théoriques et pratiques ou démonstratives. Vidéo-projection. Résumer et fiche réflexe distribués à chaque participant en fin de formation. Synthèse finale sous forme d'un jeu.
Compétences / Capacités professionnelles visées	• Comprendre les enjeux de la cybersécurité et les impacts sur l'entreprise • Comprendre et détecter les principales failles et moyens d'attaques • Adopter les bon réflexes et améliorer son hygiène informatique
Durée	7 heures
Dates	Nous consulter
Lieu(x)	Nous consulter
Coût par participant	Nous consulter



Accessibilité	 Un entretien préalable sera mis en place pour aménager au mieux la formation avec votre handicap. Nos intervenants savent adapter leurs méthodologies pédagogiques en fonction des différentes situations d'handicap.
Restauration	/
Hébergement	/
Responsable de l'action, Contact	Elise LAMIRE / formation@impi.fr / +33 5 58 06 23 23
Formateur /trice	Ludovic BLANCHARD / formation@impi.fr / +33 5 58 06 23 23
Suivi de l'action	Mise en place d'outils permettant de vérifier la réalité du suivi de la formation par les stagiaires (<i>émargement par les stagiaires et le formateur, Attestation de stage</i>) Une attestation de compétences sera remise à chaque stagiaire
Évaluation de l'action	Une évaluation de l'action (<i>satisfaction des participants</i>) et une autre sur le degré d'acquisition des compétences (<i>Mise en situation...</i>) sont à envisager. Évaluation de la prestation de formation « à chaud » (<i>tour de table, cible, bilan écrit...</i>). Évaluation des acquis au regard des objectifs attendus « à froid » <i>après 3 mois</i>