Formation
du SPN - réSeau des Professionnels du Numérique

5 rue Victor Hugo - 86000 POITIERS
www.spn.asso.fr
contact@spn.asso.fr - 05 49 03 17 76

Fil conducteur

PRÉSENTATION GÉNÉRALE / INFOS PRATIQUES

Titre de la formation	COMPRENDRE LES MENACES CYBER ET ANTICIPER VOTRE ORGANISATION EN CAS D'INCIDENT
Objectifs de la session (selon programme)	· Sensibiliser les dirigeants aux enjeux de la cybersécurité pour toutes les entreprises · Fournir des éléments de réflexion concrets et des aides pour passer à l'action. · Ouvrir l'esprit sur des bonnes pratiques organisationnelles pour gérer les risques et répondre à des incidents informatiques majeurs comme une cyberattaque
Type de formation	Présentiel avec une première partie de théorie et partage et une seconde avec des ateliers pratiques
Public / spécificités des stagiaires	Des dirigeants, salariés ou indépendants non experts informatiques ou non spécialiste cybersécurité
Accessibilité handicap :	

Prérequis exigés	néant
Méthode validation des prérequis	néant
Matériel requis	Projecteur pour l'animateur / Post IT ou Tableau numérique, Papier libre A4 et crayons pour les ateliers
Support pédagogique	Réalisé par Cybil et délivré sur place en projection
Horaires formation (amplitude journée) + pauses	Durée prévue de 7h par l'animateur dont une pause de 15mn dans la matinée et celle du déjeuner. L'après-midi étant en ateliers, un temps de pause pourra être pris.
Animation par :	Stéphane THOREL de Cybil

RYTHME / DÉCOUPAGE DES SESSIONS

Séquence Module	Notions abordées	Pour quel résultat ?	Durée	Début	Fin	Méthode pédagogique	Moyens utilisés
ACCUEIL	Tour de table et prise de contact		15	9h	9h15		
THÉORIE 1	• Statistiques et tendances actuelles des cybermenaces • Définition des enjeux de protection et activités de cybersécurité • Importance pour les entreprises de toutes tailles	Comprendre les fondamentaux de la cybersécurité.	45	9h15	10h	Informations et supports fournis par le formateur	projecteur
ATELIER 1	• Rappel par les stagiaires des menaces existantes et réflexion individuelle sur les risques qu'il identifie pour son entreprise • Atelier créatif pour imaginer les mobiles qui poussent un pirate, un concurrent ou un salarié à être malveillant • Analyse des impacts de malveillance et sur les réflexes à adopter face à des situations réelles.	Identifier les risques de chaque participant à travers un atelier collaboratif guidé.	60	10h	11h	Discussions interactives dirigées	Projecteur + fournitures
PAUSE			15	11h	11h15		
THEORIE 2	Les types de menaces et réflexes à adopter	Débrief du Cluedo Cyber et retour sur les principales menaces et réflexes à adopter.	45	11h15	12h	Discussions interactives	Projecteur
THÉORIE 3	• Coûts directs et indirects. • Obligations légales (RGPD, etc.).	Comprendre les impacts d'une	30	12h	12h30	Informations et supports	Projecteur + fournitures

	• Impacts sur la réputation et la confiance des clients.	cyberattaque sur l'entreprise.				fournis par le formateur	
DEJEUNER				12h30	13h30		
THEORIE 3	• Évaluation des risques spécifiques à chaque entreprise. • Éléments d'une politique de sécurité. • Outils pour définir les besoins en cybersécurité.	Commencer à définir une approche proactive et élaborer une stratégie de cybersécurité	60	13h30	14h30	Informations et supports fournis par le formateur	Projecteur
ATELIER 2	• Principes fondamentaux d'une charte cybersécurité. • Ateliers en petits groupes pour commencer à rédiger leur propre charte.	Formulation d'une charte de cybersécurité	60	14h30	15h30	Informations et cadre posé par l'animateur puis travail de groupe	Projecteur + fournitures
PAUSE			15	15h30	15h45		
ATELIER 3	• Stratégies de sensibilisation efficaces (formations, newsletters, affichages). • Création d'un plan de sensibilisation adapté à leur entreprise. • Échanges d'expériences sur ce qui fonctionne ou non.	Fournir des idées et des outils pour sensibiliser les employés à la cybersécurité.	60	15h45	16h45	Travail en groupe pour concevoir des initiatives concrètes et des messages clés à diffuser	Projecteur + fournitures
	• Résumé des points clés. • Discussion sur les prochaines étapes et les ressources disponibles.	Conclusion	30	16h45	17h15		

EVALUATION DES ACQUIS

À chaque session, les résultats individuels des stagiaires seront reportés sur la synthèse d'évaluation des acquis

Objectif du programme	Notion / compétence transmise	Méthode de vérification	Type de « notation »	Moyen/outil utilisé
Sensibiliser et fournir des éléments de réflexion concrets et des aides pour passer à l'action.	Avoir identifié des risques numériques liés à son activité et analyser leur impact avec des outils proposés	Implication des stagiaires et aptitude à partager les messages clés	Évaluation du formateur	Atelier pour des cas pratiques

RESSOURCES DOCUMENTAIRES DISPONIBLES

Nom de la ressource	Format	Date de découverte / mise à jour	Où le trouver ?
Présentation projetée	PowerPoint	En séance pour chaque session	Fourni par l'animateur
Supports méthodologiques pour les ateliers	PDF	En séance pour chaque session	Fourni par l'animateur
Liens internet depuis la présentation	Navigation web	En séance pour chaque session	internet