Sensibilisation à la cybersécurité

Public	MJPM en activité, autres professionnels, ou publics concernés par la protection juridique des majeurs ou œuvrant auprès des personnes en situation de vulnérabilité		
Prérequis	Publics concernés par la protection juridique des majeurs ou œuvrant auprès des personnes en situation de vulnérabilité	**Nombre de participants**	15 participants
Dates	Mercredi 17 décembre 2025	**Horaires**	14h à 17h
Lieu	Distanciel / outil Visio de la FNMJI		
Prix	Tarif adhérent FNMJI : 110.00 € HT et 110.00 € TTC Tarif Contributeurs FNMJI : 110.00 € HT et 110.00 € TTC Tarif assistant des adhérents FNMJI : 140.00 € HT et 140.00 € TTC Tarif sympathisant des associations locales futurs MJPM : 160.00 € HT et 160.00 € TTC Tarif non adhèrent FNMJI : 190.00 € HT et 190.00 € TTC		

Accessibilité handicap	La FNMJI demande à être informée sur les situations de handicap des participants afin d'adapter les modalités pédagogiques aux objectifs de la formation, de prendre en compte les moyens de compensation du handicap. *Contact Référent Handicap : formation@fnmji.fr*

Moyens d'encadrement pédagogique et technique	**Intervenant**	M laurent MONNIER, Administrateur système & réseau
	Responsable pédagogique	FNMJI
	Responsable de projet	Cécile CARDUNER formation@fnmji.fr

Source et bibliographie	• L'ANNSI • Cybermalveillance.gouv • Guides essentiels et bonnes pratiques de cybersécurité
Modalités d'évaluation des acquis	Un questionnaire sur les attentes de participants est envoyé en amont, avec possibilité d'analyse de dossiers spécifiques illustrant la formation. Une évaluation pédagogique est transmise à chaque participant par mail à la fin de la formation. Deux mois plus tard, un questionnaire d'évaluation pédagogique est transmis à chaque participant par mail. Un bilan oral peut être réalisé à l'issue de la session de formation.
Sanction de la formation	Une attestation individuelle de formation sera transmise à chaque participant à l'issue de la formation.

Programme de formation

Objectifs pédagogiques	Contenus pédagogiques	Méthodes pédagogiques
Installer le processus de formation Créer la dynamique du groupe de formation	Présentation réciproque Consignes de fonctionnement et de rythme	Mise en place de la formation Outil Visio FNMJI
Identifier les principaux types de menaces numériques et comprendre leurs mécanismes	**Comprendre les cyberattaques** (phishing, malwares/ransomware, attaques réseau, ingénierie sociale)	Études de cas réels, démonstrations d'attaques simulées, discussions interactives
Savoir appliquer des mesures de protection concrètes et adaptées	**Maîtriser les techniques de protection** (mots de passe robustes, authentification forte, mises à jour, sauvegardes 3-2-1, antivirus)	Exercices pratiques (création de mots de passe, configuration d'authentification MFA), ateliers de mise à jour sécurisée, tests de restauration de sauvegardes
Développer une culture de cybersécurité au sein de l'organisation	**Sensibilisation et organisation interne** (exercices de simulation, évaluation continue)	Jeux de rôle, quiz interactifs, mises en situation de phishing
Être capable d'identifier les nouveaux risques liés à l'IA et adapter la posture de sécurité	**Anticiper les risques liés à l'IA** (exploitation malveillante, deepfakes, attaques automatisées	Démonstration, analyses de scénarios
Connaître les obligations légales et réglementaires et aligner la stratégie de sécurité avec ces cadres	**Normes et réglementations** (RGPD, recommandations ANSSI, directive NIS2)	Analyse de textes réglementaires, ateliers de conformité, étude comparative
Comprendre pourquoi la cybersécurité est vitale et mobiliser les parties prenantes	**Importance de la cybersécurité pour l'entreprise** (enjeux financiers, réputationnels, continuité d'activité)	Présentation illustrée, analyse de cas d'entreprises attaquées, brainstorming collectif
Evaluer la formation	Bilan oral	Bilan oral
	Recueil des attentes spécifiques	Questionnaire De satisfaction adressé par mail le jour de la formation