



 DURÉE 1 jour 7h	 FORMAT Intra Visio Présentiel	 PRÉREQUIS Aucun	 ÉQUIPEMENT Ordinateur
---	--	--	--


DÉLAIS D'ACCÈS
 Les inscriptions sont ouvertes jusqu'à 15 jours avant le début de la formation, sous réserve de places disponibles.


ACCESSIBILITÉ
 Nous nous adaptons pour répondre aux besoins spécifiques de chaque situation de handicap.


Pour qui ?

Professionnels de la communication, responsables marketing, chefs de projet en communication d'influence



Mise en pratique

Édition des bonnes pratiques pour une campagne d'influence



Personnalisation

Chaque formation est adaptée en fonction de votre niveau, en termes de contenu et durée



Moyens pédagogiques et techniques

- Accueil des stagiaires dans une salle équipée pour le présentiel
- Documents de formation projetés (vidéos - PowerPoint)
- Exposés théoriques, études de cas et exemples
- Mise en pratique



Suivi et évaluation de la formation

- Feuilles de présence signées par demi-journée
- Questionnaire de positionnement en amont
- Évaluation finale et QCM de contrôle des acquis
- Débriefing collectif en fin de session



Objectifs

- Pour dirigeants & managers : Comprendre les risques et l'approche Zero Trust, sécuriser l'entreprise avec des protections adaptées (firewall, antivirus), adopter les bonnes pratiques contre le phishing et les cyberattaques, maîtriser les obligations RGPD et impliquer les collaborateurs via une charte et des formations
- Pour employés : Identifier les cybermenaces (phishing, social engineering), appliquer les bonnes pratiques au travail et à domicile, sécuriser les données personnelles selon le RGPD, intégrer le Zero Trust et signaler toute anomalie, avec des mises en situation et un quizz interactif



Programme

- Etat des risques
- Les bonnes pratiques au travail (phishing, social engineering, matériel inconnu mots de passe...)
- Les bonnes pratiques au domicile (IOT, réseau personnel, VPN d'entreprise, anti virus)
- RGPD, la protection des données personnelles et leur importance, le DPO
- L'importance du zero trust
- L'importance de remonter l'information (doute, suspicion, attaque avérée...)
- Exemple d'attaques, interaction
- Evolution des risques informatiques
- Rappel du Zero trust
- jeu quizz interactif et rappel des règles
- Rappel des bonnes pratiques au travail et à la maison