

Deepfakes, synthèse vocale et IA : protéger la communication de son entreprise

Lien : https://innov-maroc.com/formation/deepfakes-synthese-vocale-et-ia-proteger-la-communication-de-son-entreprise

DURÉE
5 jours (35h)

RÉFÉRENCE
COM166

CATÉGORIE
Communication Augmentée par l'IA, GenAI et Automatisation

INNOV MAROC

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre les technologies de Deepfake, de clonage vocal et de génération de contenus par IA
- Identifier les risques liés à l’usurpation d’identité des dirigeants et collaborateurs
- Reconnaître les principaux signaux permettant de détecter un contenu manipulé
- Comprendre les nouveaux scénarios de fraude utilisant la synthèse vocale et les contenus générés par IA
- Mettre en place des procédures d’authentification des communications sensibles
- Sécuriser les échanges impliquant des instructions financières, confidentielles ou stratégiques
- Protéger l’image, la voix et l’identité numérique des dirigeants et porte-paroles
- Préparer une réponse efficace face à la diffusion d’un faux contenu
- Sensibiliser les collaborateurs aux risques d’usurpation et développer une culture de vérification
- Construire une stratégie globale de prévention, détection et gestion des incidents liés aux Deepfakes et à l’IA

POUR QUI ?

- Directeurs Généraux et dirigeants d’entreprise
- Directeurs de la Communication et responsables Communication
- Responsables Communication de crise
- Responsables Marketing et Brand Managers
- Responsables Relations Presse et Affaires Publiques
- RSSI et responsables cybersécurité
- DSI et responsables transformation digitale
- Responsables Risques et Compliance
- Responsables Juridiques et Protection des données
- Community Managers et Social Media Managers
- Assistantes de Direction et collaborateurs travaillant avec des dirigeants
- Responsables RH et responsables de la sensibilisation interne
- Professionnels souhaitant protéger la réputation, l’identité numérique et les communications stratégiques de leur organisation

INOV MAROC



Programme détaillé

1 / Comprendre les menaces liées aux Deepfakes et à l'IA

- Comprendre le fonctionnement des deepfakes, clonages vocaux et contenus générés par IA
- Identifier les risques pour l'image, la réputation et la communication de l'entreprise
- Analyser les nouveaux scénarios de fraude et d'usurpation d'identité

2 / Identifier les techniques de manipulation multimédia

- Reconnaître les principales techniques de falsification vidéo, audio et image
- Identifier les indices visuels, vocaux et contextuels suspects
- Comprendre les limites des méthodes traditionnelles de vérification

3 / Détecter les Deepfakes vidéo et audio

- Analyser les anomalies de synchronisation labiale et d'expression
- Identifier les incohérences dans la voix, le rythme et les intonations
- Utiliser des outils d'analyse et de détection adaptés

4 / Protéger l'identité numérique des dirigeants

- Identifier les risques liés au clonage de voix et à la reproduction d'image
- Sécuriser les prises de parole publiques et contenus institutionnels
- Définir des règles d'utilisation et de diffusion des contenus sensibles

INNOV MAROC

5 / Prévenir les fraudes par usurpation vocale

- Identifier les scénarios de fraude au président et de fausse instruction
- Mettre en place des procédures de vérification avant toute action sensible
- Sécuriser les demandes financières ou confidentielles transmises par téléphone ou messagerie

6 / Mettre en place un protocole d'authentification des communications

- Définir des mécanismes permettant de vérifier l'identité d'un interlocuteur
- Mettre en place des procédures de double validation
- Définir des canaux officiels pour les communications critiques

7 / Protéger la communication de crise et la réputation

- Préparer un dispositif de réaction face à un faux contenu viral
- Organiser la vérification, qualification et escalade d'un incident
- Construire une stratégie de communication permettant de préserver la confiance

8 / Sécuriser les contenus générés par IA de l'entreprise

- Définir les règles d'utilisation de l'IA générative pour les communications
- Identifier les risques de diffusion d'informations confidentielles
- Mettre en place des processus de validation humaine des contenus sensibles

9 / Sensibiliser les collaborateurs et les dirigeants

- Former les équipes à reconnaître les tentatives d'usurpation
- Développer des réflexes de vérification face aux demandes inhabituelles
- Organiser des simulations de scénarios de fraude et de deepfake

10 / Construire un plan de défense contre les menaces IA

- Cartographier les risques liés aux deepfakes et à l'usurpation numérique
- Définir les rôles, responsabilités et procédures d'intervention

INOV MAROC

- Mettre en place une démarche continue de veille, prévention, détection et réponse

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Mises en Situation pour faciliter l'assimilation
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

07 au 11 Déc. 2026	Présentiel - Casablanca
04 au 08 Jan. 2027	Présentiel - Casablanca
01 au 05 Mars 2027	Présentiel - Casablanca
26 au 30 Avr. 2027	Présentiel - Casablanca
21 au 25 Juin 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-maroc.com
Web : https//www.innov-maroc.com

INNOV MAROC

INNOV MAROC — Tous droits réservés