FORMATION

FORMATION – CYBERVIGILANCE & CYBERMALVEILLANCE : DÉVELOPPER LES BONS RÉFLEXES DE CYBERSÉCURITÉ

Théâtre à la Carte Digital Generation

Mise à jour 2026

OBJECTIFS PÉDAGOGIQUES

Former les collaborateurs aux réflexes essentiels de cybersécurité afin de :
• Comprendre les risques cyber auxquels l'entreprise est exposée
• Identifier les comportements vulnérables et les techniques de manipulation
Réagir efficacement face à une tentative d'attaque
• Adopter durablement les bonnes pratiques numériques

TOUT PUBLIC

PRÉSENTIEL, DISTANCIEL OU MIXTE
12 STAGIAIRES MAXIMUM

CONTACTEZ-NOUS POUR SÉLÉCTIONNER DES DATES DE FORMATION

FORMAT CLASSIQUE :
1 COMÉDIEN FORMATEUR, SAYNÈTES EN VIDÉO, JUSQU'À 3 MISES EN SITUATION.

1600 EUROS

FORMAT PREMIUM :
2 COMÉDIENS FORMATEURS, SAYNÈTES JOUÉES EN LIVE, JUSQU'À 5 MISES EN SITUATION.

2200 EUROS

AUCUN PRÉREQUIS N'EST DEMANDÉ POUR PARTICIPER À CETTE FORMATION

MOYENS PÉDAGOGIQUES

- Saynètes
- Vidéos
- Apports théoriques et pratiques
- Mises en situation
- Echanges interactifs
- Présentation Powerpoint
- Plateforme LMS

Les moyens et supports mobilisés sont employés en fonction des besoins identifiés lors du questionnaire de positionnement.

Nos formateurs sont des experts de la thématique et reconnus dans le métier : consultez leur profil dans notre CVthèque accessible en ligne.

Certification non concernée

CONTENU DE LA FORMATION

Axe 1 – Sensibiliser aux risques cyber du quotidien

Tour de table : usages numériques et perception des risques cyber
Saynète théâtrale : "Le clic de trop"
Débriefing collectif avec les participants :
Quels signaux d'alerte étaient visibles ?
Pourquoi le personnage s'est-il laissé piéger ?
Comment aurions-nous réagi à sa place?
Quels réflexes adopter au quotidien ?

Identification des situations à risque dans le quotidien professionnel : mots de passe faibles, clics sur des liens frauduleux, partage d'informations sensibles, utilisation des outils IA sans vigilance, connexions non sécurisées…

Décryptage des principales cybermenaces : phishing, ransomware, fraude au président, usurpation d'identité, fuite de données, cyberharcèlement

Axe 2 – Comprendre les mécanismes de la cybermalveillance

Définition des notions de cybersécurité, cybermalveillance et ingénierie sociale
Focus sur les nouvelles menaces liées à l'intelligence artificielle
Statistiques et exemples concrets de cyberattaques en entreprise
Rôle et responsabilité des collaborateurs dans la protection des données et des systèmes

Axe 3 – Réagir efficacement et adopter les bons réflexes

Atelier pratique reconnaître un mail frauduleux, sécuriser ses mots de passe, détecter les manipulations émotionnelles
Mise en situation : appel suspect, tentative d'usurpation, clé USB piégée, faux support informatique, usage imprudent d'un outil d'IA
Activité collaborative : « Que faire si une attaque survient ?
Procédures d'alerte et remontée d'incidents
Techniques de communication pour alerter un collègue ou refuser une demande douteuse
Construction d'une culture collective de cybervigilance

Axe 4 – Ancrer une culture cybersécurité dans l'entreprise

Comprendre que la cybersécurité est l'affaire de tous
Développer les réflexes de vigilance collective
Identifier les leviers d'engagement et de responsabilisation
Créer des habitudes durables grâce à des rappels simples et concrets
Engagement individuel : chaque participant repart avec ses " 3 réflexes cyber "
ACCOMPAGNEMENT POST FORMATION EN OPTION