

GWENDAL LE COGUIC

FORMATIONS

Chaque formation est axée sur des démonstrations pratiques, des exercices interactifs et des discussions sur des situations réelles afin de garantir l'acquisition de compétences clés.

Chaque session peut être suivie :

- sur site ou à distance
- en français ou en anglais
- individuellement ou en groupe

Devis sur demande

Tel: +33 7 69 02 25 10

Email: contact@glc.st

SENSIBILISATION À LA CYBERSÉCURITÉ



a. Description

*Cette formation de sensibilisation d'une journée s'adresse à tous les **employés et collaborateurs** qui interagissent quotidiennement avec les outils numériques. L'objectif est de **démystifier** la cybersécurité, de présenter les **principales menaces et risques** auxquels les organisations sont confrontées aujourd'hui et de fournir aux participants des connaissances concrètes et pratiques pour réduire les vulnérabilités. Grâce à des **explications claires**, des **exemples concrets** et des **conseils pratiques**, cette session contribue à créer une culture de responsabilité partagée en matière de sécurité de l'information.*

b. Objectifs pédagogiques

- Comprendre les principales menaces en cybersécurité et leur impact
- Identifier les techniques d'attaque courantes
- Reconnaître l'importance du comportement des utilisateurs dans la prévention des incidents
- Appliquer les bonnes pratiques au quotidien
- Réagir de manière appropriée face à des incidents de sécurité potentiels
- Comprendre les responsabilités légales et organisationnelles

c. Pré-requis

Aucun.

d. Public cible

- Collaborateurs de tous niveaux : managers et chefs d'équipe, ressources humaines, personnel administratif...
- Support informatique et équipes techniques

- Télétravailleurs

e. Programme

Introduction à la cybersécurité

- Qu'est-ce que la cybersécurité et son importance ?
- Exemples concrets de menaces
- Importance du comportement utilisateur

Rôles et responsabilités organisationnels

- Qui fait quoi en cybersécurité ?
- Partage des responsabilités et coopération interservices
- Sensibilisation aux risques et communication interne

Contexte juridique et réglementaire

- Aperçu du RGPD et des autres réglementations clés
- Ce que dit la loi sur la protection des données et la réponse aux incidents
- Obligations individuelles et conformité des entreprises

Paysage des menaces et scénarios d'attaque

- Cybermenaces courantes
- Études de cas et incidents réels
- Comprendre le facteur humain dans les cyberattaques

Bonnes pratiques pour un comportement sécurisé

- Hygiène des mots de passe et authentification multifacteur
- Sécurité des e-mails et identification des tentatives de phishing
- Navigation et utilisation des réseaux sociaux en toute sécurité

Sécurisation des outils et environnements numériques

- Utilisation sécurisée des appareils (ordinateurs, téléphones, clés USB)
- Télétravail sécurisé
- Sauvegarde des données et mises à jour logicielles

Réagir à un cyber incident

- Détecter et signaler les activités suspectes
- Mesures immédiates à prendre en cas de faille de sécurité
- Construire un plan d'action sur mesure

Synthèse et recommandations

- Résumé des points clés
- Ressources pour rester informé
- Discussion ouverte et questions-réponses