LEXORA
LE SAVOIR DE L'EXPERT

Réf. LEX-CYB-003
Formacode 31006
Version LEX-CYB-003_v1.0 · MAJ
Généré le 11/08/2026

Sensibilisation de vos équipes aux cybermenaces

Vos collaborateurs sont le premier rempart contre les cyberattaques, mais aussi le premier vecteur d intrusion. En 1 jour, formez-les aux bons reflexes.

ESSENTIEL | IA & DIGITAL | 1 jour (7h)

INFORMATIONS PRATIQUES

Référence	**LEX-CYB-003**
Formacode	**31006**
Durée	**1 jour (7h)**
Version	**LEX-CYB-003_v1.0 · MAJ**

Une question ?
Contenu, financement, organisation — réponse sous 24h.

contact@darkcyan-bat-723962.hostingersite.com
05 54 07 30 33

LE CONSTAT

En 2024, 91 % des cyberattaques commencent par un email de phishing (Verizon DBIR, 2024). La sensibilisation des equipes reduit les incidents de 70 %.

NOTRE RÉPONSE

En 1 jour, vos equipes acquierent les reflexes de base pour detecter et reagir aux cybermenaces.

Source : Verizon - Data Breach Investigations Report (DBIR), 2024

POUR QUI

PUBLIC CIBLE
Equipes et collaborateurs de TPE-PME, managers, assistants, commerciaux souhaitant adopter les bons reflexes cyber.

PRÉREQUIS
Aucun prerequis. Formation destinee aux equipes, pas aux techniciens.

Délai d'accès : 14 jours ouvres avant la session

LES BÉNÉFICES DE LA FORMATION

Concrètement, après cette formation

- ✓ Vos equipes reconnaissent les emails de phishing avant de cliquer
- ✓ Chaque collaborateur applique les 10 reflexes cyber au quotidien
- ✓ Vous avez une procedure de signalement et de reaction claire
- ✓ Vous reduisez le risque d incident cyber de 70 %

OBJECTIFS PÉDAGOGIQUES

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

1. Reconnaitre les principales cybermenaces (phishing, ransomware, ingenierie sociale) et leurs vecteurs d attaque
2. Appliquer les 10 reflexes de cybersecurite dans son travail quotidien (mots de passe, emails, navigation, cles USB)
3. Detecter une tentative de phishing ou d arnaque au president et appliquer la procedure de signalement
4. Reagir correctement en cas d incident de securite en suivant la procedure d alerte de l entreprise

PROGRAMME DÉTAILLÉ

Le programme sur 1 jour (7h)

MOD-SEC-001 — MOD-SEC-001 - Comprendre les cybermenaces — 2h

- Panorama des menaces. Cas reels d attaques sur des PME. Les consequences pour l entreprise et le collaborateur. Les vecteurs d attaque.

MOD-SEC-002 — MOD-SEC-002 - Les 10 reflexes cyber — 2h

- Mots de passe forts et gestionnaire. Double authentification. Mises a jour. Sauvegardes. Navigation securisee. Wi-Fi public. Cles USB. Verrouillage de session. Reseaux sociaux. BYOD.

MOD-SEC-003 — MOD-SEC-003 - Detecter les attaques — 1h30

- Reconnaitre un phishing : les 7 signaux. Arnaque au president. Ingenierie sociale au telephone. Simulation de phishing.

MOD-SEC-004 — MOD-SEC-004 - Reagir en cas d incident — 1h30

- Les 5 premieres minutes apres un incident. Procedure de signalement. Qui contacter. Documentation. Plan d action equipe.

MODALITÉS PÉDAGOGIQUES

Notre approche

MÉTHODE
Cas réels
Cas reels et exercices pratiques. Format 8 max.

FORMAT
8 max
Interaction garantie avec le formateur

MOYENS
Support + outils
Presentiel : salle equipee. Distanciel : Zoom. Support PDF, outils, acces replay 30 jours.

RATIO
75% pratique
Vérifié sur scénario minuté

75% Pratique — cas réels, QCM, échanges — 25% Théorie

Moyens techniques — Presentiel : salle equipee. Distanciel : Zoom. Support PDF, outils, acces replay 30 jours.

FORMATEUR RÉFÉRENT

Sebastien Hurstel
Consultant digital

Consultant digital, Sebastien forme les equipes aux reflexes cyber avec une pedagogie accessible et des exercices realistes.

Cette formation peut également être animée par tout formateur qualifié par LEXORA.

ACCESSIBILITÉ

Formation accessible PSH

Adaptation sur demande.
Référent : William Bigot
accessibilite@darkcyan-bat-723962.hostingersite.com
0612225849

ÉVALUATION

Comment nous mesurons vos acquis

AVANT
Questionnaire de positionnement

PENDANT
Exercices pratiques + QCM par bloc

APRÈS
Evaluation a chaud + attestation de competences

Suivi de l'exécution — Feuilles d emargement signees par demi-journee, attestation d assiduite, certificat de realisation.

☆ PARCOURS PRÉ & POST-FORMATION

J+7
Email recapitulatif + ressources

J+14 - J+42
1 defi pratique / semaine pendant 4 semaines

J+30
Evaluation a froid + feedback formateur

J+60
Webinaire Q&A Retour terrain

TARIFS

MODALITÉ	FORMAT	TARIF
Sur-mesure		*Cette formation est disponible en intra-entreprise sur mesure.*