CYBE-001

Hygiène numérique

Programme de formation professionnelle en cybersécurité — 1 journée pour acquérir les bons réflexes et protéger votre organisation des cybermenaces du quotidien.

Informations générales

Fiche programme

Code : CYBE-001

Durée : 7 heures (1 jour)

Modalité : Présentiel ou distanciel

Public : Tous collaborateurs, aucun prérequis technique

Effectif : 6 à 12 participants

Référentiel : RGPD art. 32 — NIS2

Financement éligible

Cette formation est finançable dans le cadre du **Plan de Développement des Compétences (PDC)** via les OPCO suivants :

- OPCO 2i
- Atlas
- OPCO Santé
- Opcommerce
- Constructys
- Afdas
- AKTO

Accompagnement dans la constitution du dossier de financement inclus.

Objectifs pédagogiques

À l'issue de la formation, le participant sera capable de :

1	**Identifier les cybermenaces** Reconnaître les attaques courantes ciblant les collaborateurs : phishing, ransomware, ingénierie sociale.
2	**Sécuriser ses mots de passe** Mettre en place une gestion robuste des mots de passe et activer l'authentification à deux facteurs.
3	**Naviguer en sécurité** Adopter les bons réflexes de navigation web et de gestion de la messagerie professionnelle.
4	**Protéger ses données** Sécuriser ses données en situation de mobilité : déplacement, télétravail, cloud.
5	**Réagir aux incidents** Savoir réagir et alerter efficacement en cas d'incident de sécurité avéré ou suspecté.

Module 1 — Les cybermenaces du quotidien

DURÉE : 1H30

Phishing & ingénierie sociale

Reconnaître les tentatives de phishing, spear-phishing et manipulation psychologique utilisées par les attaquants pour obtenir des informations sensibles.

Malwares & logiciels espions

Identifier les vecteurs d'infection courants : pièces jointes, clés USB, sites compromis, et comprendre comment ces logiciels opèrent discrètement.

Ransomware

Comprendre comment les rançongiciels se propagent dans les systèmes d'information et les mesures concrètes pour s'en protéger efficacement.

Cas réels commentés

Analyse d'exemples d'attaques récentes en entreprise pour ancrer les apprentissages dans des situations concrètes et mémorables.

Module 2 — Mots de passe et authentification

DURÉE : 1H30

Contenu du module

Mots de passe robustes

Créer et gérer des mots de passe forts selon les recommandations ANSSI : longueur, complexité, unicité.

Gestionnaire de mots de passe

Découvrir et utiliser un gestionnaire de mots de passe pour centraliser et sécuriser ses accès sans effort mémoriel.

Authentification 2FA

Mettre en place et utiliser l'authentification à deux facteurs sur les comptes professionnels et personnels sensibles.

🔧 Atelier pratique

Audit de ses mots de passe actuels

Chaque participant analyse en binôme la robustesse de ses mots de passe existants et identifie les comptes à risque à sécuriser en priorité.

Livrable : Liste personnelle des comptes à sécuriser en priorité

Module 3 — Messagerie et navigation sécurisée

DURÉE : 2H

Identifier un email ou lien suspect

Analyser les indices révélateurs d'un message frauduleux : expéditeur, URL, ton d'urgence, demandes inhabituelles. Développer un regard critique systématique.

Bonnes pratiques de navigation web

Vérifier le protocole HTTPS, gérer les extensions de navigateur, éviter les réseaux Wi-Fi publics non sécurisés et utiliser un VPN en déplacement.

Pièces jointes et téléchargements

Gérer les pièces jointes avec discernement : formats à risque, vérification de l'expéditeur, analyse avant ouverture, politique de téléchargement sécurisé.

🎭 Atelier pratique : jeux de rôle

Analyse d'emails suspects en situation simulée. Les participants jouent alternativement le rôle de l'attaquant et de la cible pour mieux comprendre les mécanismes de manipulation.

Module 4 — Données, mobilité et réaction aux incidents

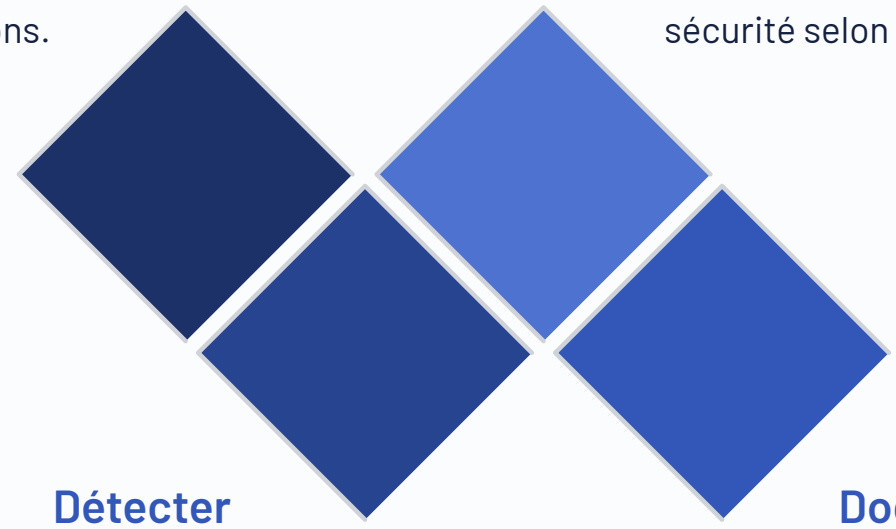
DURÉE : 2H

Contenir

Isoler l'appareil et couper les connexions.

Alerter

Contacter le responsable sécurité selon l'escalade.



Détecter

Identifier rapidement les signes de compromission.

Documenter

Consigner les faits pour l'analyse post-incident.

En cas de suspicion d'incident, chaque minute compte. Ce module donne aux collaborateurs les réflexes concrets pour limiter l'impact d'une compromission.

Protection en mobilité

- Sécurisation des appareils mobiles (chiffrement, verrouillage)
- Usages du cloud personnel vs. professionnel : les règles à respecter
- Bonnes pratiques en télétravail et lors des déplacements professionnels

Chaîne d'escalade

- Qui prévenir en cas d'incident ?
- Dans quel délai alerter ? (obligations RGPD : 72h)
- Comment documenter l'incident pour faciliter l'analyse

Livrable : Checklist de sécurité personnelle remise à chaque participant à l'issue du module.

Méthodes pédagogiques

Apports théoriques

Contenus illustrés de cas réels récents pour ancrer les apprentissages dans des situations concrètes vécues en entreprise.

Quiz de positionnement

Évaluation initiale en début de session pour adapter le niveau des échanges au profil réel des participants.

Ateliers en binôme

Analyse d'emails suspects et audit de mots de passe en situation pratique, favorisant l'apprentissage par l'expérience directe.

Livrables participants

Checklist de sécurité personnelle et procédure de signalement remises à chaque participant à l'issue de la formation.

Évaluation finale

QCM de validation des acquis en fin de session avec score minimum requis de 70% pour l'obtention de l'attestation.

Votre formateur

Alexandre BOIGUES

Formateur indépendant spécialisé en cybersécurité
NDA 11 92 27843 92

Ingénieur système de formation et ex-CTO, Alexandre intervient depuis **10 ans** auprès d'organisations de toutes tailles pour les accompagner dans leur montée en compétences en sécurité numérique.

Références clients

AG2R	BNP Paribas
Orano	CHU Rouen

Expertises & veille

- Ingénierie système & architecture sécurité
- Expérience CTO en environnement exigeant
- Membre actif **CyberV**
- Veille permanente **ANSSI / CERT-FR / CNIL**

Modalités d'évaluation

- Quiz de positionnement initial
- QCM final — score minimum : **70%**
- Attestation individuelle de formation

Contact & tarifs

Telemach Learning

📧 alexandre@telemach-learning.fr

📞 +33 6 66 88 75 63

📍 24 Rue Chanzy, 92600 Asnières-sur-Seine

🌐 www.telemach-learning.fr

Tarif intra-entreprise : Sur devis selon effectif et modalité (présentiel / distanciel)

Financement OPCO / PDC

Cette formation est éligible au financement via votre OPCO dans le cadre du Plan de Développement des Compétences.

Nous vous accompagnons dans **la constitution complète de votre dossier de financement** pour simplifier vos démarches administratives.

Conformité assurée : **RGPD art. 32** et directive **NIS2** — référentiels intégrés au programme.

Demander un devis | **En savoir plus**