Cybersécurité et IA - Bonnes Pratiques Quotidiennes

Mathieu CHEVILLARD

Objectifs de la journée

Comprendre les menaces

Comprendre les menaces cyber actuelles en 2026

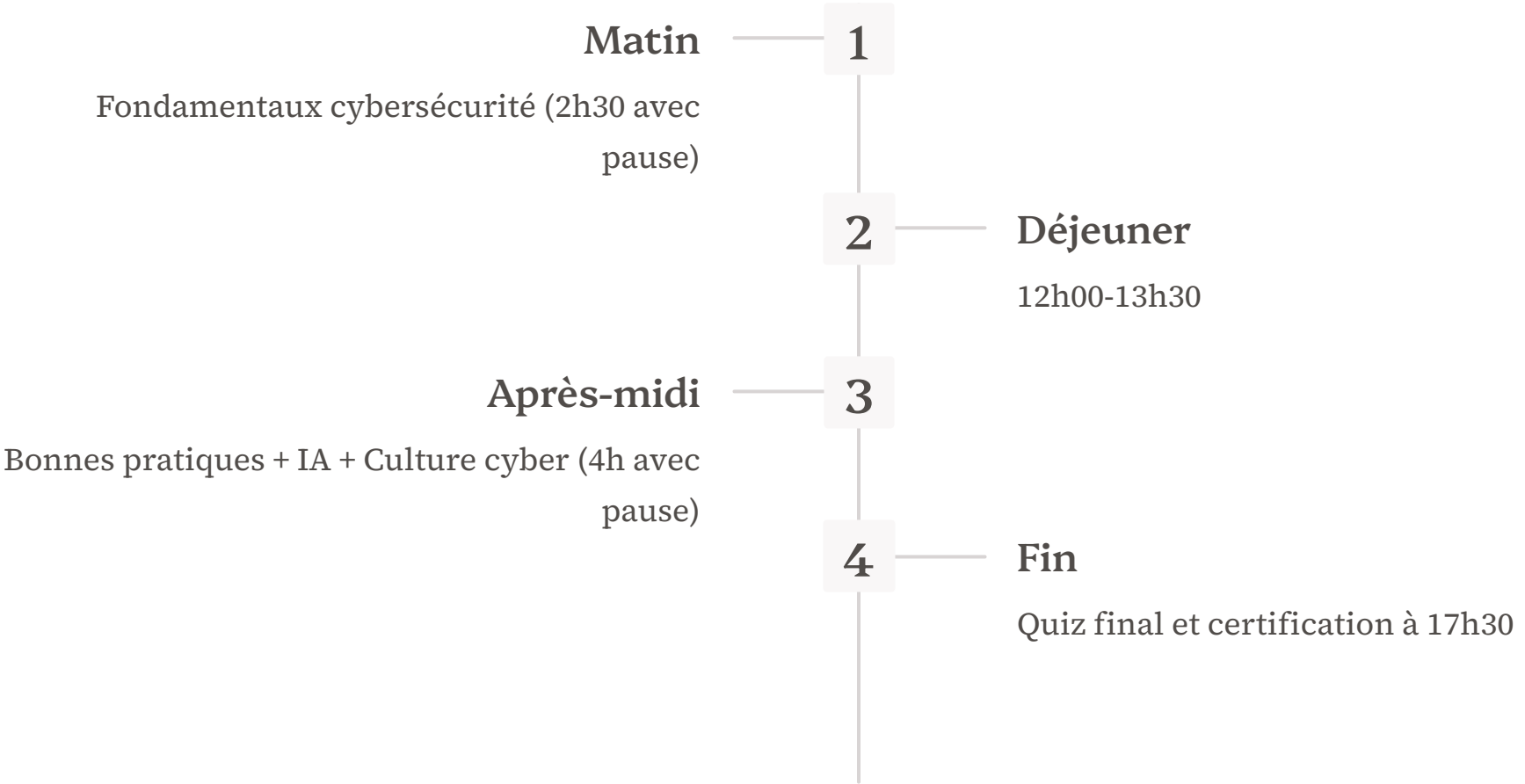
Adopter les bons réflexes

Adopter les bons réflexes au quotidien

Protéger les données

Protéger les données de l'entreprise et ses clients

Déroulement de la journée - Planning complet avec horaires



Modalités pédagogiques

Format interactif et participatif

Format interactif et participatif

Quiz interactifs

Quiz interactifs pour ancrer les apprentissages

Ateliers pratiques

Ateliers pratiques (phishing, IA)

Certification

Certification de participation

Présentations et tour de table

- Qui êtes-vous ?
- Quelles sont vos attentes ?
- Niveau d'expérience en cybersécurité

Module 1 - Fondamentaux Cybersécurité (Slides 6-18)

Les enjeux de la cybersécurité en 2026

80%

Entreprises victimes

80% des entreprises victimes d'au moins une cyberattaque par an

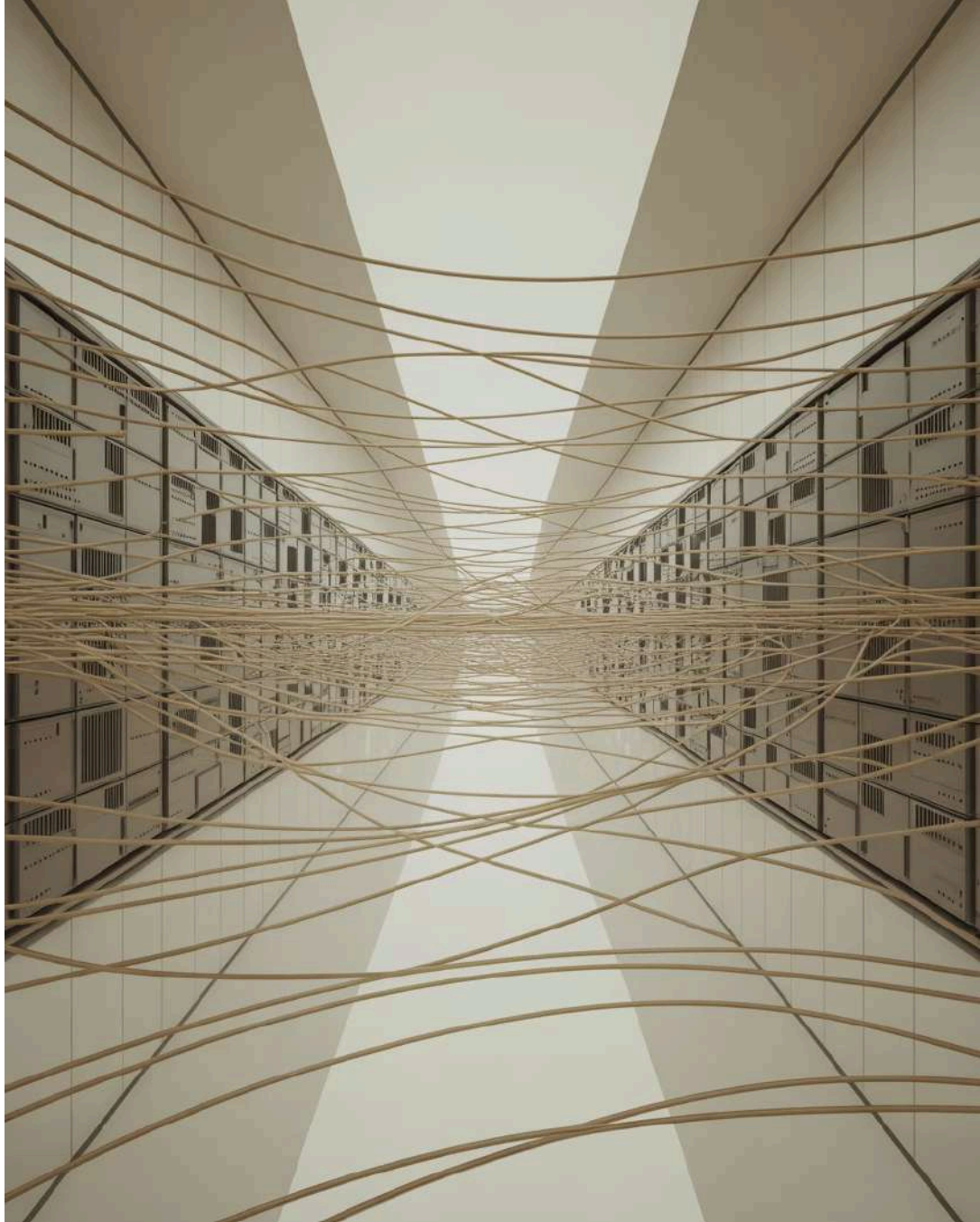
4,45M€

Coût moyen

Coût moyen d'une violation : 4,45M€

Le télétravail augmente la surface d'attaque

La cybersécurité = responsabilité de TOUS



Panorama des menaces

Phishing

90% des cyberattaques commencent par un email

Ransomware

chiffrement et demande de rançon

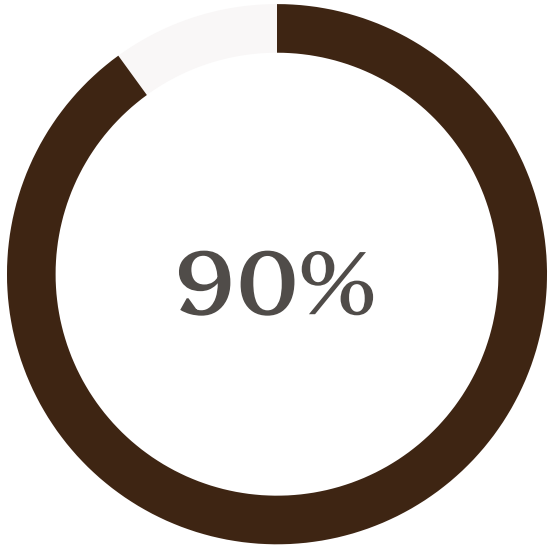
Malware

virus, chevaux de Troie, spywares

Attaques ciblées

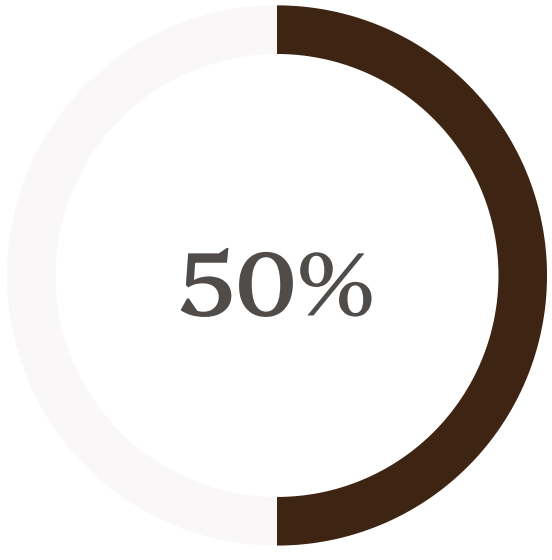
ingénierie sociale, APT

Le facteur humain



Erreur humaine

90% des incidents liés à l'erreur humaine



Réduction des risques

La formation réduit les risques de 50%

L'employé = première ligne de défense

Les mots de passe - Règles d'or

01

Longueur et complexité

Minimum 12 caractères (majuscules, minuscules, chiffres, symboles)

02

Unicité

UN mot de passe UNIQUE par compte/service

03

Gestionnaire

Utiliser un gestionnaire de mots de passe

04

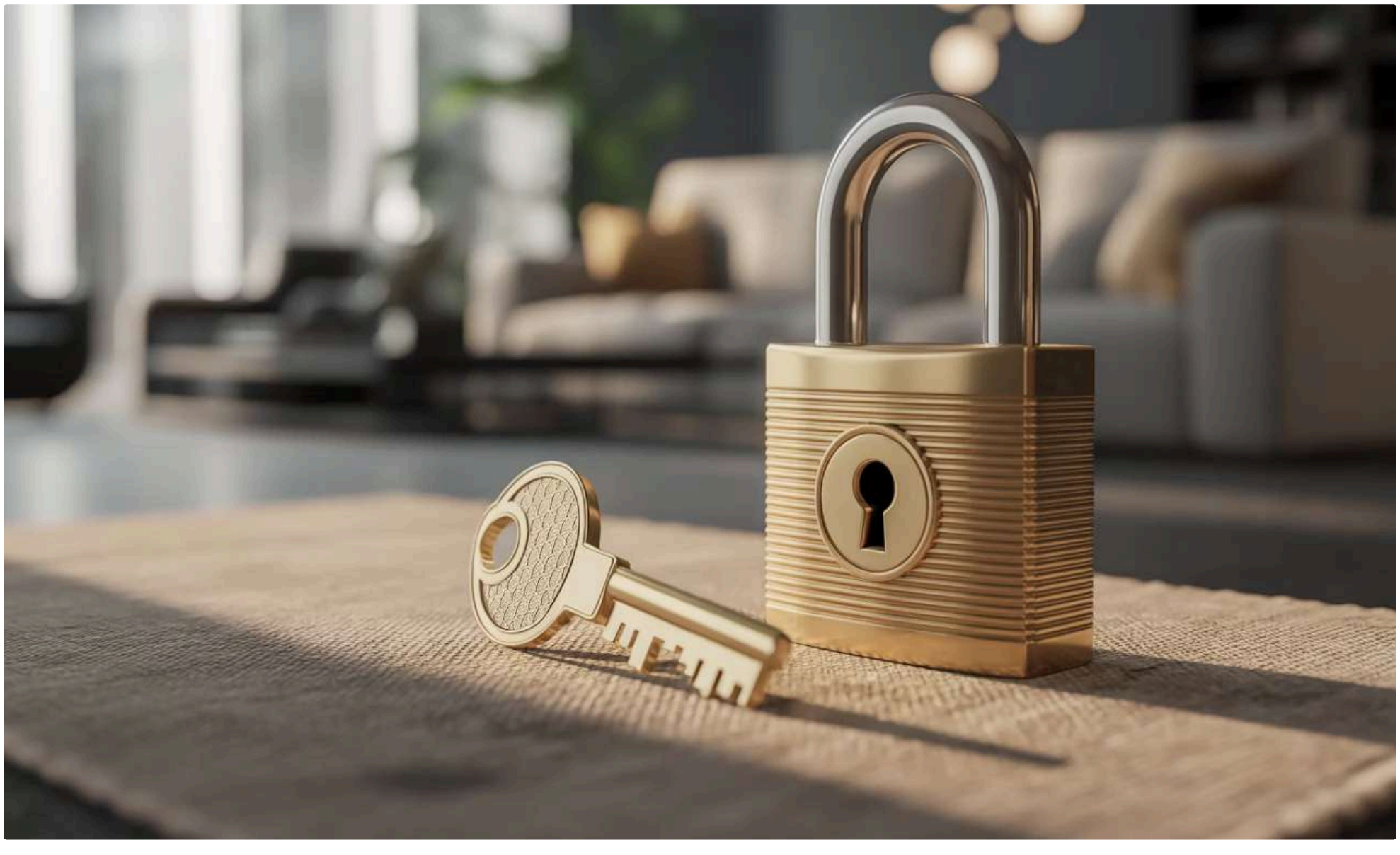
Confidentialité

Ne JAMAIS partager son mot de passe

05

Changement

Changer immédiatement si suspicion de compromission



L'authentification multifacteur (MFA/2FA)

Une 2ème vérification après le mot de passe

Méthodes

Code SMS, application (Google Authenticator), biométrie

Efficacité

Réduit de 99,9% le risque de piratage de compte

Activation

À activer PARTOUT où c'est proposé

Indispensable pour : messagerie, banque, cloud, RH, VPN

Le phishing - Reconnaître les signaux d'alerte

1

Expéditeur suspect

Expéditeur inconnu ou adresse email suspecte

2

Fautes

Fautes d'orthographe et grammaire approximative

3

Urgence

Sentiment d'urgence ou menace

4

Demande d'infos

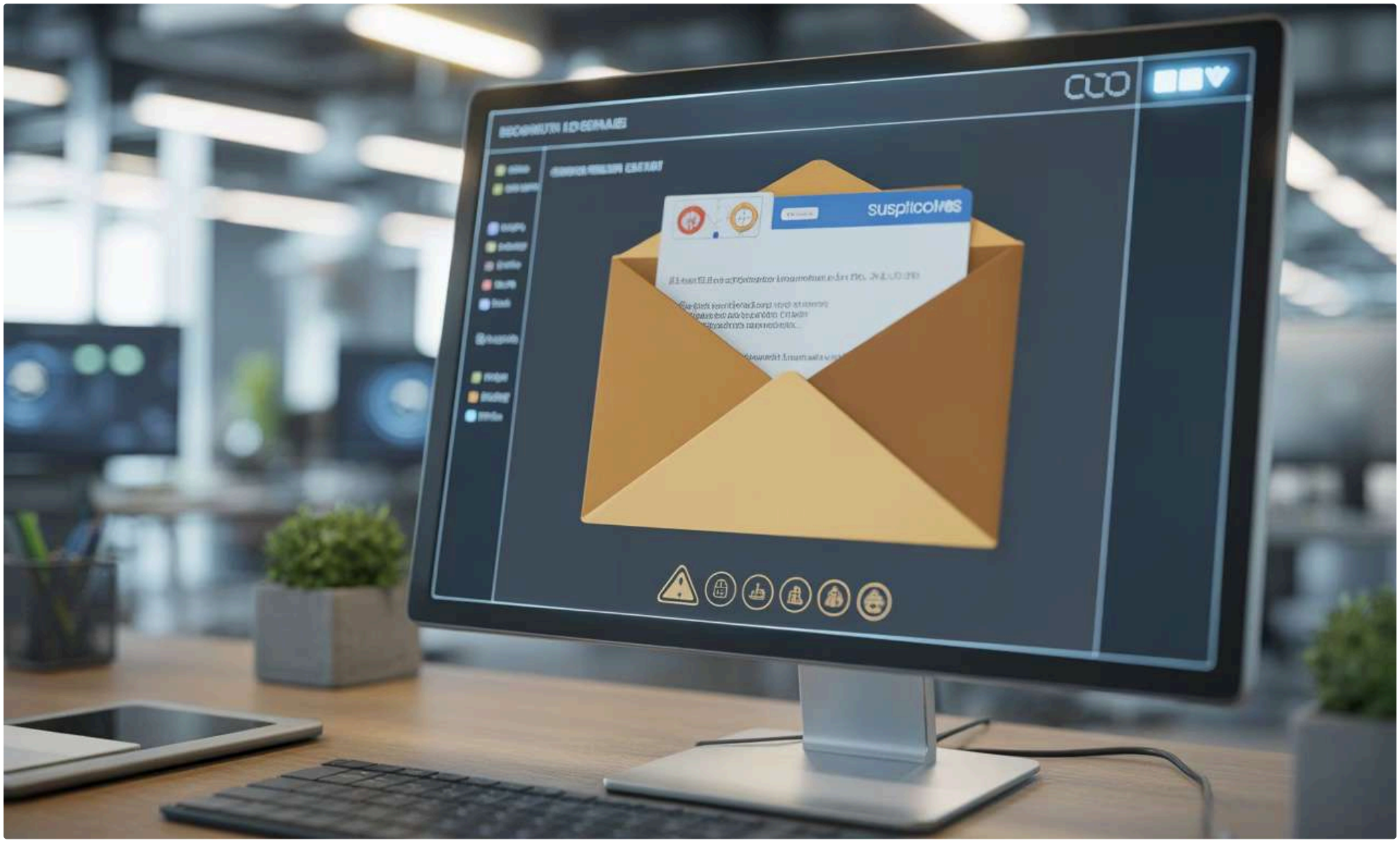
Demande d'informations confidentielles

5

Lien ou PJ

Lien ou pièce jointe non sollicités

EN CAS DE DOUTE : NE PAS CLIQUER - Signaler au service IT



Les mises à jour - Pourquoi sont-elles critiques

Failles corrigées

Corrigent les failles de sécurité exploitées par les hackers

Mise à jour immédiate

À faire IMMÉDIATEMENT pour : Windows, applications, navigateurs, antivirus

Automatisation

Activer les mises à jour automatiques

Un logiciel non mis à jour = porte ouverte aux pirates

Les sauvegardes - La règle 3-2-1

3

Copies

3 copies de vos données importantes

2

Supports

2 supports différents (disque dur externe + cloud)

1

Hors site

1 copie hors site (cloud sécurisé)

Fréquence : hebdomadaire minimum (quotidien pour données critiques)

Tester régulièrement la restauration

Protection des équipements : Antivirus, Pare-feu, VPN

ANTIVIRUS

Détecte et bloque les malwares (à jour obligatoire)

PARE-FEU

Filtre le trafic réseau entrant/sortant

VPN

Chiffre la connexion (obligatoire en WiFi public et télétravail)

Tous les appareils doivent être protégés

Ne jamais désactiver ces protections

Le RGPD et la protection des données personnelles

Données personnelles : nom, email, RH, clients, fournisseurs

Principes

Minimisation, finalité, durée limitée, sécurité

Obligations

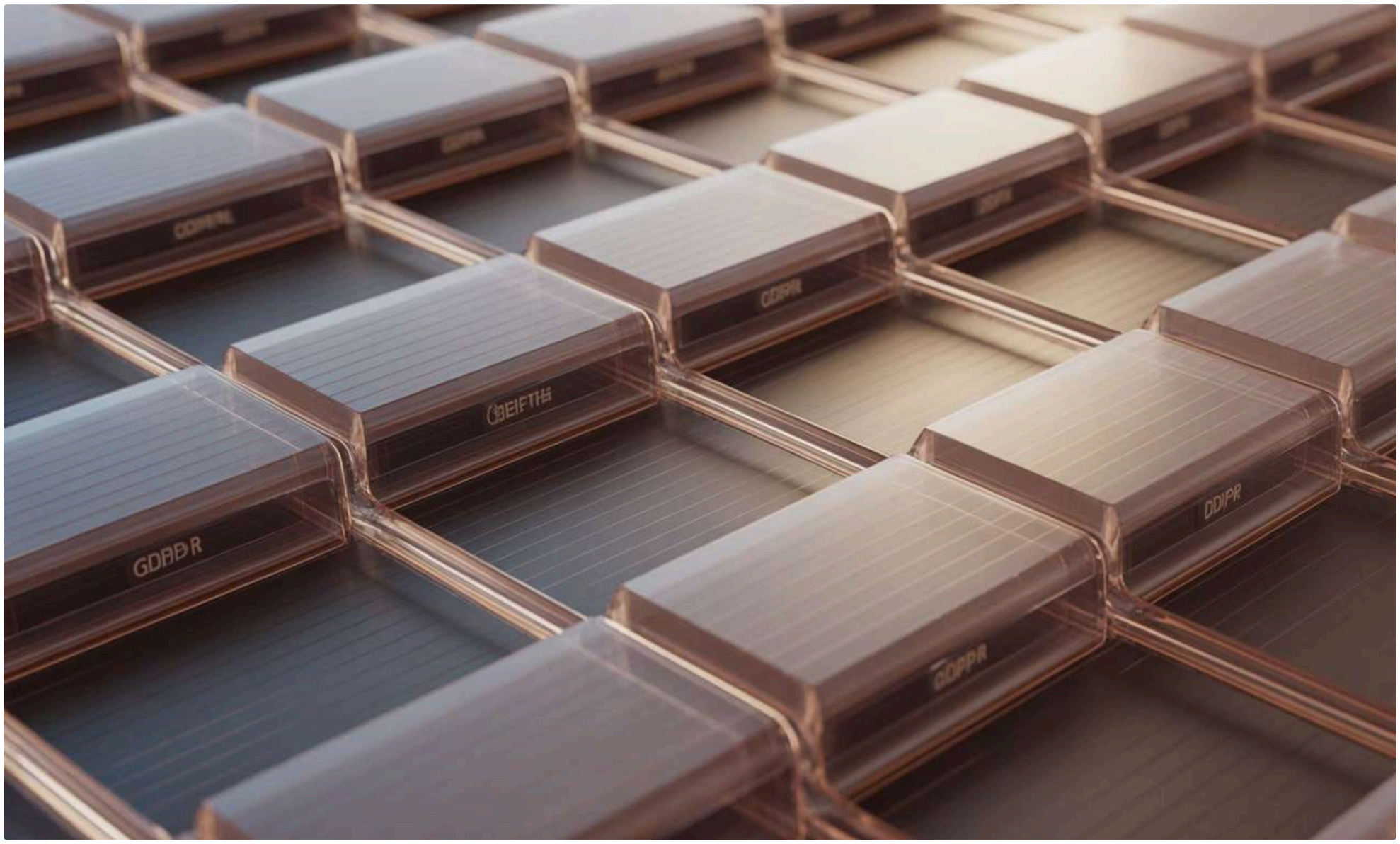
Ne collecter que le nécessaire, protéger, informer

Sanctions

jusqu'à 20M€ d'amende

Votre rôle

Protéger TOUTES les données que vous traitez



La séparation vie pro/vie perso - BYOD

Règles de base

- Ne pas mélanger équipements personnels et professionnels
- Si BYOD autorisé : exigences de sécurité strictes
- Séparer les messageries pro/perso
- Respecter la charte informatique de l'entreprise

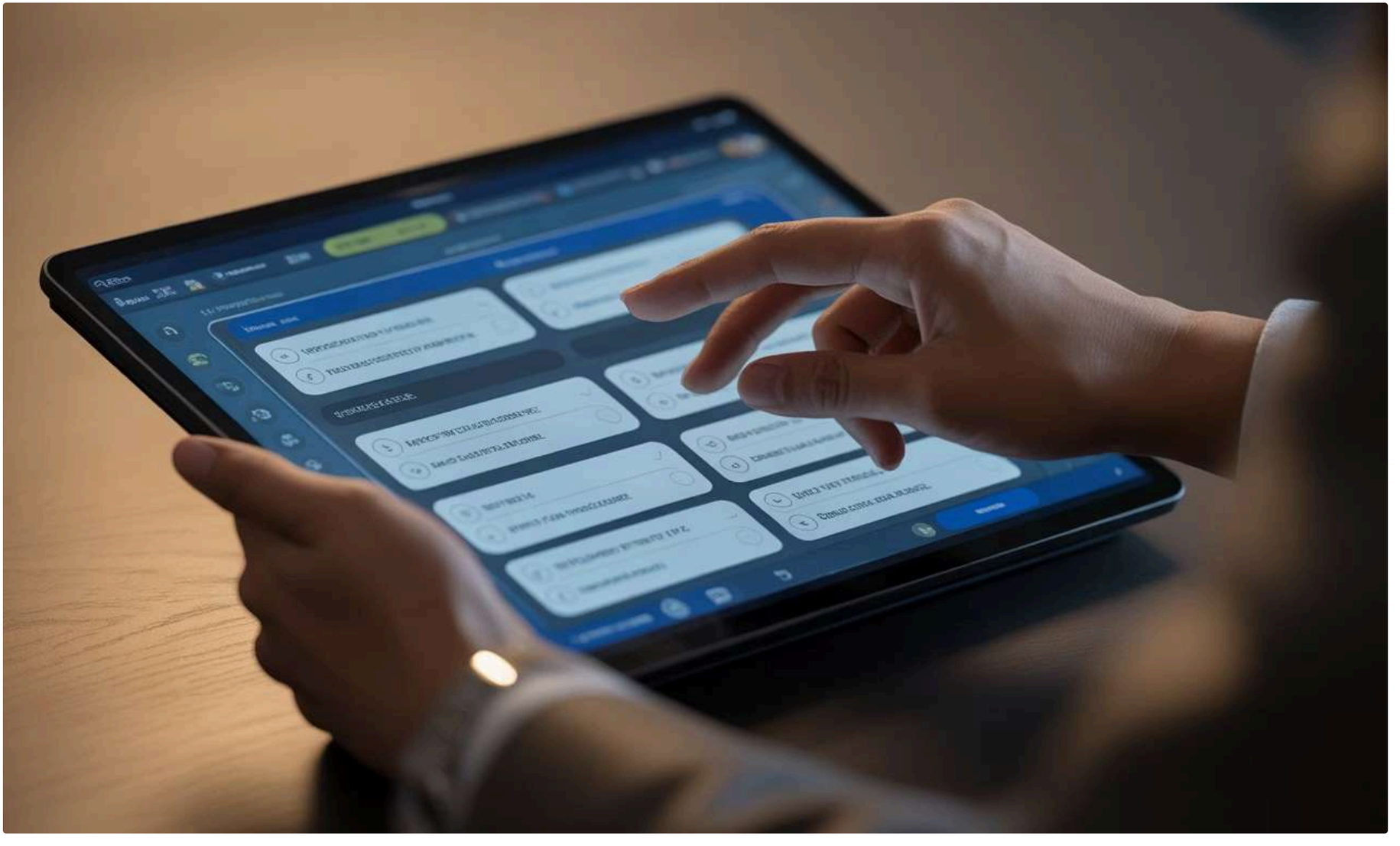
PAUSE CAFÉ

(10h30-10h45)

Retour à 10h45 pour le quiz

Quiz interactif - Évaluation des connaissances Module 1

Questions à choix multiples et scénarios pratiques



🍽 PAUSE DÉJEUNER

12h00-13h30 (1h30)

Retour à 13h30 précises pour la reprise de l'après-midi

Module 2 - Bonnes Pratiques Quotidiennes (Slides 20-30)

13h30-15h00 (1h30)

Reprise après-midi - Les 10 réflexes cyber du quotidien

- Verrouiller son poste dès qu'on s'éloigne (Win+L)
- Vérifier l'expéditeur avant d'ouvrir un email
- Ne jamais cliquer sur un lien/PJ suspect
- Utiliser des mots de passe forts et uniques
- Activer la MFA partout
- Faire les mises à jour immédiatement
- Sauvegarder régulièrement ses données
- Utiliser un VPN sur les réseaux publics
- Séparer vie pro et vie perso
- Signaler tout incident au service IT

Sécuriser son poste de travail

Verrouillage automatique

Écran verrouillé automatiquement après inactivité

Bureau propre

Bureau propre : pas de post-it avec mots de passe

Accès physique

Accès physique sécurisé (badge, bureau fermé)

Protection matérielle

Câble antivol pour portables

Destruction sécurisée

Destruction sécurisée des documents sensibles

Naviguer en toute sécurité

→ HTTPS

Vérifier le cadenas HTTPS avant de saisir des données

→ Publicités

Ne pas cliquer sur les publicités douteuses

→ Téléchargements

Télécharger uniquement depuis sites officiels

→ Bloqueur

Utiliser un bloqueur de publicités

→ Nettoyage

Effacer historique et cookies régulièrement

Gérer ses emails avec vigilance

Vérification expéditeur

Vérifier l'adresse exacte de l'expéditeur

Pas de réponse

Ne pas répondre aux emails suspects

Survol des liens

Survoler les liens sans cliquer pour voir l'URL réelle

Pièces jointes

Attention aux pièces jointes inattendues

Signalement

Utiliser la fonction "Signaler comme phishing"

Télétravailler en sécurité

Matériel professionnel

Utiliser UNIQUEMENT le matériel professionnel pour le travail

VPN obligatoire

Se connecter via VPN pour accéder aux ressources entreprise

WiFi sécurisé

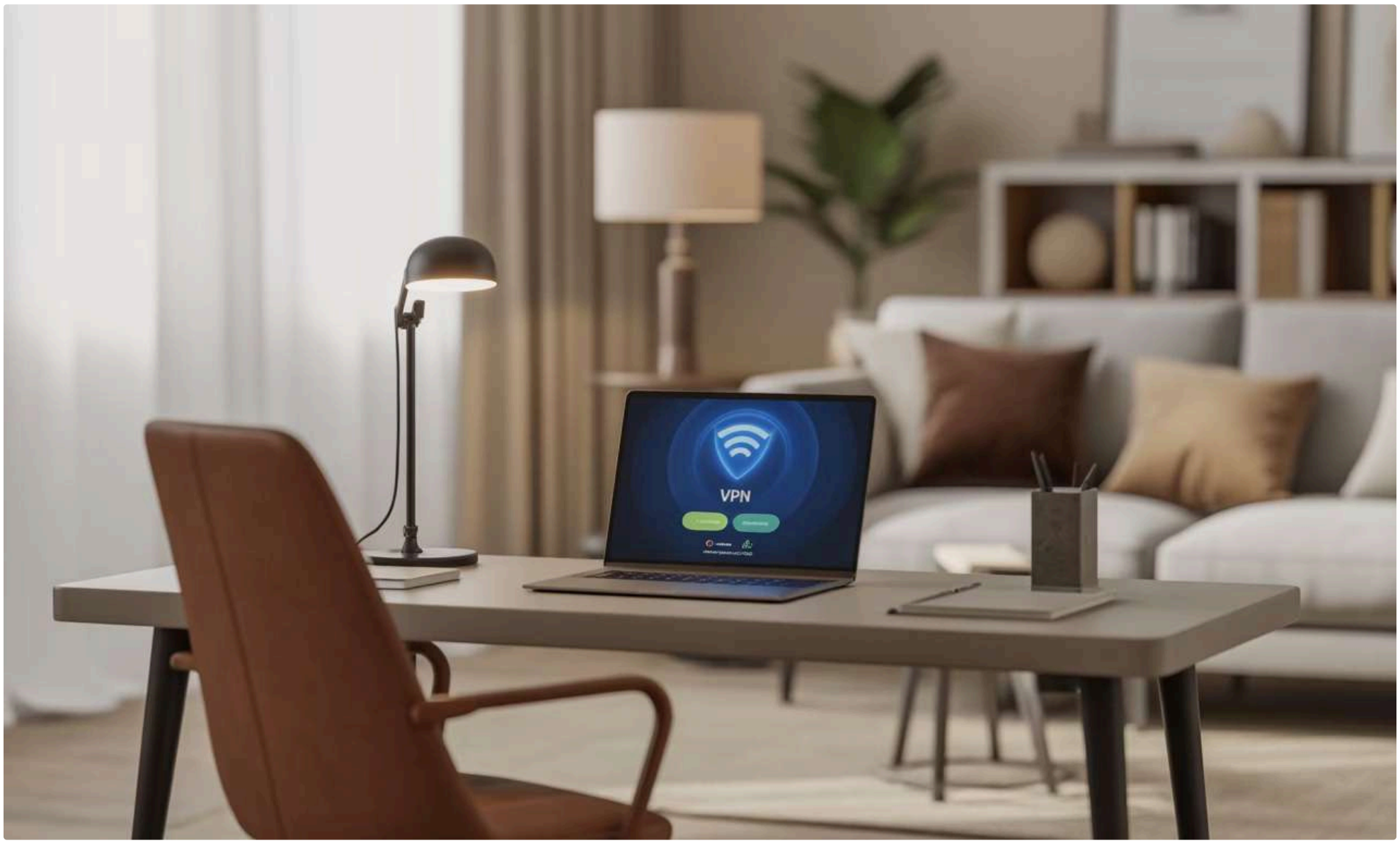
WiFi sécurisé avec mot de passe fort (WPA3 si possible)

Confidentialité écran

Écran non visible par des tiers

Verrouillage

Verrouiller systématiquement l'ordinateur



Utiliser les réseaux WiFi publics

1

VPN obligatoire

TOUJOURS utiliser un VPN sur WiFi public

2

Pas de comptes sensibles

Ne jamais accéder à des comptes sensibles (banque, RH)

3

Désactiver partage

Désactiver le partage de fichiers

4

Oublier le réseau

Oublier le réseau après utilisation

5

Privilégier 4G/5G

Privilégier la 4G/5G si possible

Protéger ses données en mobilité

Protections techniques

- Chiffrement complet du disque dur activé
- Localisation à distance et effacement activés
- Sauvegardes régulières avant les déplacements

Comportements sécurisés

- Ne jamais laisser l'appareil sans surveillance
- Éviter les bornes USB publiques (juice jacking)

Réseaux sociaux et e-réputation professionnelle

1. **Séparation**
   Séparer comptes professionnels et personnels

2. **Confidentialité**
   Paramètres de confidentialité au maximum

3. **Informations sensibles**
   Ne jamais partager d'informations confidentielles de l'entreprise

4. **Connexions**
   Attention aux demandes de connexion suspectes

5. **Vérification**
   Vérifier avant de publier

Que faire en cas d'incident

RÉAGIR

Déconnecter immédiatement du réseau si compromission

SIGNALER

Contacter le service IT/RSSI sans délai

NE PAS

Payer de rançon, tenter de réparer seul

DOCUMENTER

Noter heure, symptômes, actions effectuées

CONTACTS

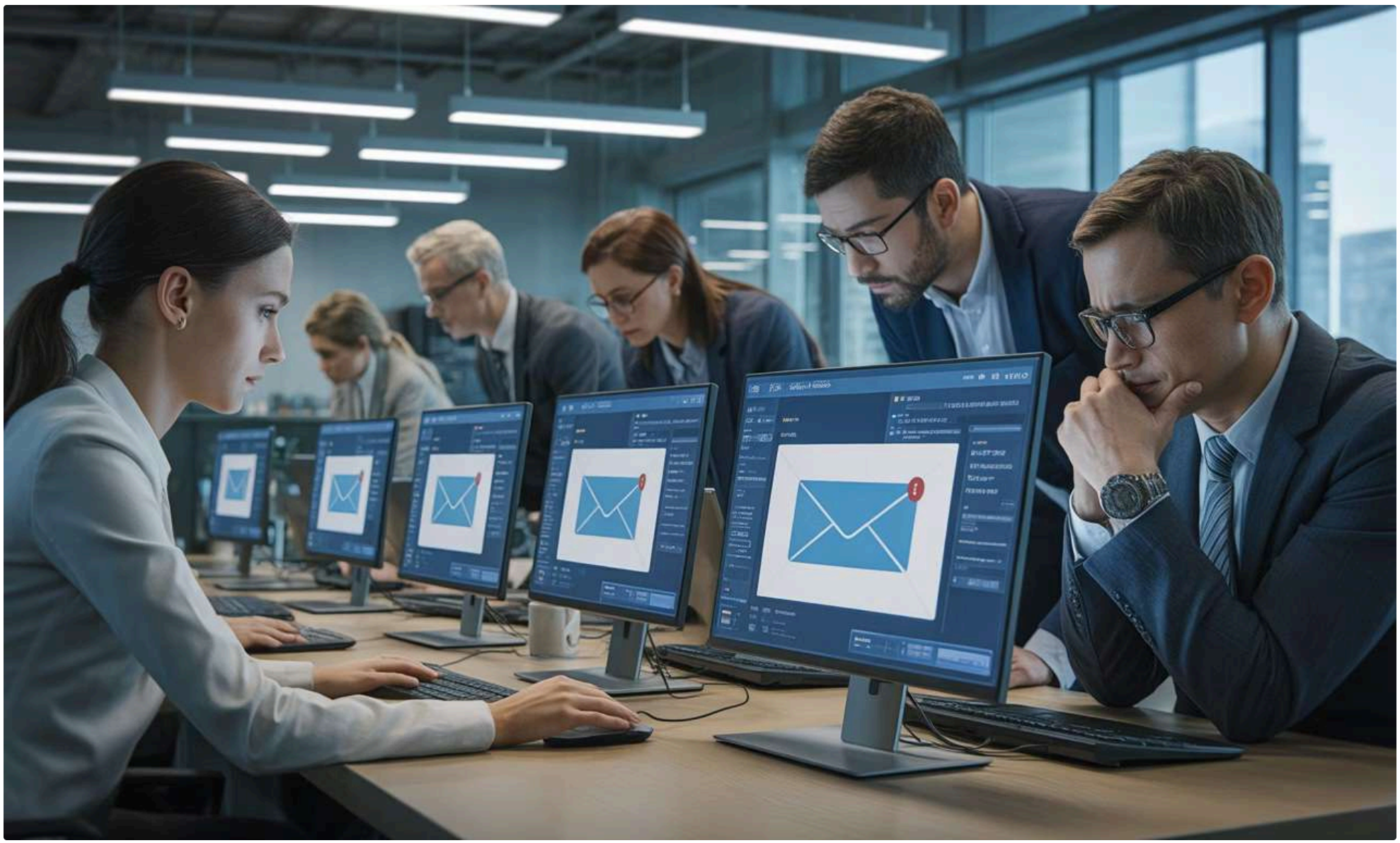
Numéros d'urgence IT affichés

🎯 ATELIER PRATIQUE

Simulation de détection de phishing

(20 min)

Analyser 5 emails et identifier les vrais/faux - Exercice interactif



Débriefing atelier phishing

Correction collective

Correction collective

Analyse des erreurs

Analyse des erreurs communes

Retour d'expérience

Retour d'expérience des participants

Points de vigilance

Points de vigilance à retenir

Module 3 - IA et Cybersécurité (Slides 31-40)

15h00-16h30 (1h30)

L'IA générative - Opportunités et risques

Opportunités

Productivité, créativité, automatisation

Risques

Fuites de données, Shadow AI, dépendance

L'IA n'est pas infaillible : hallucinations possibles

Utilisation encadrée obligatoire en entreprise

ChatGPT, Copilot, Gemini - Usages professionnels sécurisés

Utiliser UNIQUEMENT les versions validées par l'entreprise

❌ NE JAMAIS saisir

données clients, RH, financières, code source, stratégie

✅ Vérification obligatoire

Vérifier TOUJOURS les informations générées

✅ Utiliser pour

brainstorming, rédaction générique, formation

✅ Respect de la charte

Respecter la charte IA de l'entreprise

Les nouveaux risques liés à l'IA

DEEPFAKES

Vidéos/audios ultra-réalistes de dirigeants (fraudes)

MANIPULATION

Génération de faux emails, documents très crédibles

FUITES DE DONNÉES

Tout ce qui est saisi peut être stocké/réutilisé

PHISHING ASSISTÉ PAR IA

Emails personnalisés et sans faute

SHADOW AI

Utilisation non autorisée d'outils IA = risque majeur

Charte d'utilisation de l'IA en entreprise

01

Définition des usages

Usages autorisés vs interdits clairement définis

02

Validation préalable

Validation préalable obligatoire pour tout nouvel outil IA

03

Gestion des accès

Gestion des accès et permissions

04

Formation obligatoire

Formation obligatoire avant utilisation

05

Sanctions

Sanctions en cas de non-respect

Prompts et confidentialité - Ce qu'il ne faut JAMAIS partager

❌ INTERDIT

- Noms et coordonnées de clients/fournisseurs
- Données RH des collaborateurs
- Chiffres financiers de l'entreprise
- Stratégie commerciale ou projets confidentiels
- Code source, mots de passe, identifiants
- Tout document classifié 'confidentiel' ou 'interne'

✅ AUTORISÉ

Principes généraux, demandes génériques anonymisées

PAUSE

(15h45-16h00)

Retour à 16h00 pour la suite du module IA

L'IA au service de la cybersécurité

Détection automatisée

Détection automatisée des menaces et anomalies

Analyse comportementale

Analyse comportementale en temps réel

Réponse accélérée

Réponse aux incidents accélérée

Threat Intelligence

Threat Intelligence et veille automatisée

Conformité

Conformité réglementaire (RGPD, DORA, NIS2)

Les attaques assistées par IA

Phishing hyperpersonnalisé

Phishing hyperpersonnalisé à grande échelle

Malwares polymorphes

Création automatisée de malwares polymorphes

Exploitation zero-day

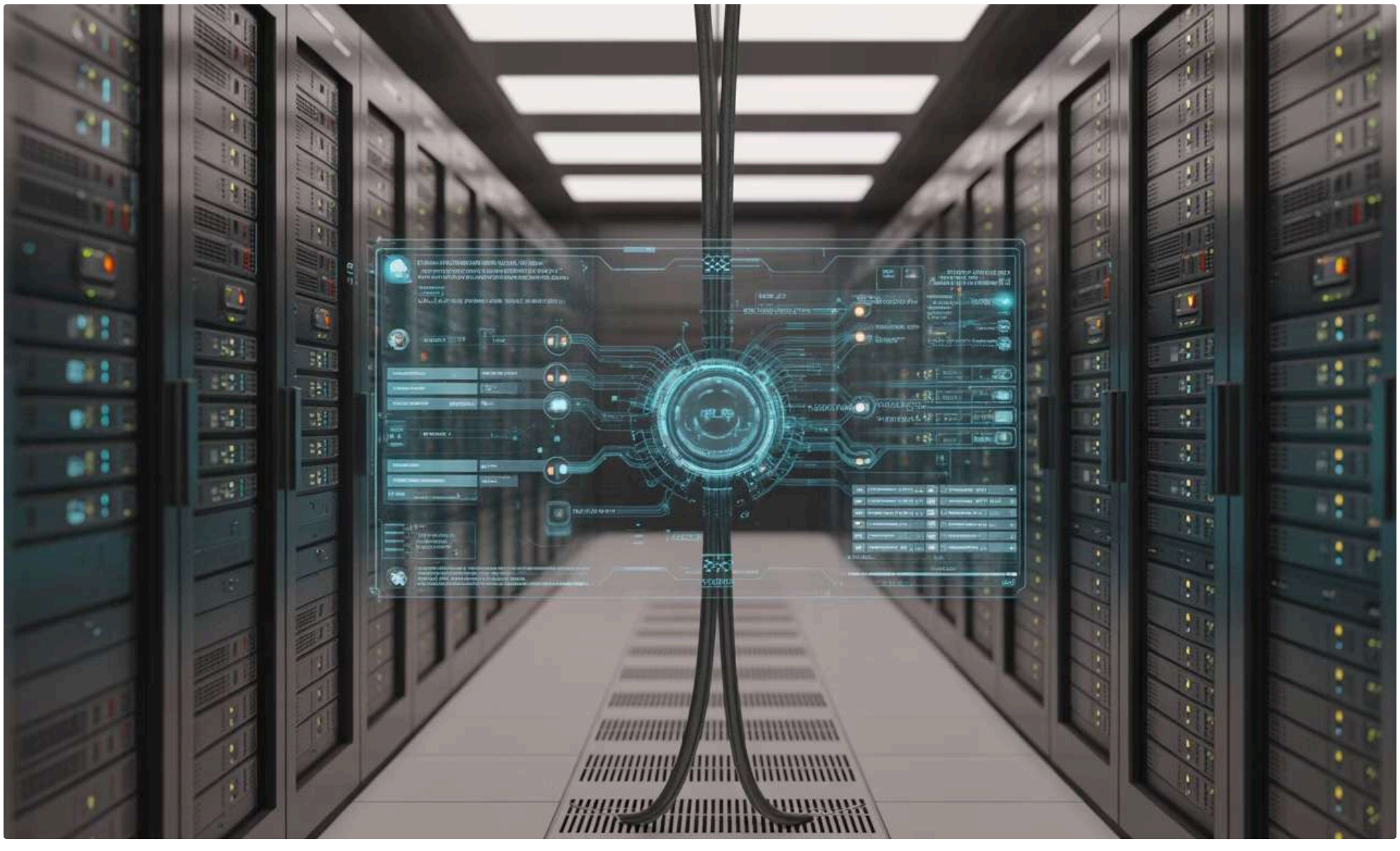
Exploitation accélérée des vulnérabilités zero-day

Contournement

Contournement des systèmes de détection

Course à l'armement

Course à l'armement IA offensive vs défensive



Bonnes pratiques - Utiliser l'IA de façon responsable

Validation humaine

Validation humaine systématique des résultats

Transparence

Transparence : indiquer quand l'IA est utilisée

Limitation

Limitation des prises de décision 100% IA

Documentation

Documentation des usages IA

Éthique

Éthique et responsabilité au cœur des usages

🎯 ATELIER

Analyse de cas d'usage IA sécurisés vs risqués

(15 min)

5 scénarios à classer : autorisé / interdit / à valider - Discussion collective

Module 4 - Culture Cyber et Engagement (Slides 41-45)

16h30-17h15 (45 min)

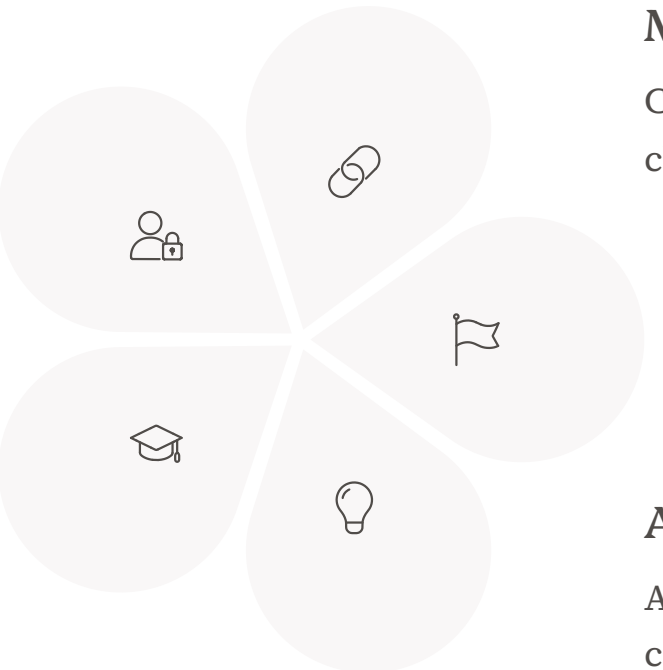
Développer une culture de cybersécurité collective

Affaire de tous

La cybersécurité = AFFAIRE DE TOUS (pas que de l'IT)

Formation continue

Sensibilisation continue et formation régulière



Maillon de la chaîne

Chaque collaborateur = maillon de la chaîne de protection

Culture du signalement

Culture du signalement sans peur de sanction

Apprentissage collectif

Apprendre de ses erreurs collectivement

Le rôle de chaque collaborateur - Ambassadeur cyber

Vigilance

Être vigilant dans ses pratiques quotidiennes

Programme ambassadeur

Programme ambassadeur cyber : devenez volontaire

Partage

Partager les bonnes pratiques avec ses collègues

Signalement

Signaler les anomalies et incidents

Participation

Participer aux formations et sensibilisations

Signaler un incident - Procédure et contacts clés

QUI contacter

Service IT, RSSI, Manager

QUAND

Immédiatement, sans délai

COMMENT

Email, téléphone, plateforme dédiée

QUOI

Décrire symptômes, heure, actions effectuées

Pas de sanction pour signalement de bonne foi

Formation continue et sensibilisation régulière

1 **Formation initiale**

Formation initiale + rappels trimestriels

2 **Simulations**

Simulations de phishing régulières

3 **E-learning**

E-learning accessible 24/7

4 **Newsletters**

Newsletters cyber mensuelles

5 **Événements**

Journées de sensibilisation (Cybermois octobre)

Les 5 actions prioritaires à mettre en œuvre DÈS DEMAIN

1

Activer la MFA

✅ Activer la MFA sur votre messagerie professionnelle

2

Mises à jour

✅ Vérifier que vos appareils sont à jour

3

Sauvegarde

✅ Créer une sauvegarde de vos données critiques

4

Mots de passe

✅ Changer les mots de passe faibles ou réutilisés

5

Charte

✅ Lire et signer la charte informatique de l'entreprise

Conclusion et Certification (Slides 46-49) - 17h15-17h30 (15 min)

Slide 46 : 📝 Quiz final de validation (10 questions)
QCM pour valider les acquis de la journée

Slide 49 : Ressources complémentaires, contacts et clôture

- **Ressources** : Guide ANSSI, Cybermalveillance.gouv.fr, fiches mémo
- **Contacts** : Service IT, RSSI, DPO
- **Support** : Présentation PDF, fiches pratiques
- **Merci pour votre participation !**