Vytalx

Check-list : programme de sensibilisation IT

Structurer une sensibilisation continue : campagnes, preuves, indicateurs
(30 minutes)

Vytalx

Comment utiliser cette checklist ?

Cochez chaque point selon votre situation.
L'objectif étant d'identifier rapidement les points d'amélioration
et de prioriser les actions qui permettent une sensibilisation efficace

Mode d'emploi

1. **Choisissez une cible :**
   (nouveaux arrivants, fonctions sensibles, IT/admins, terrain), canaux (email, Teams, micro-learning, ateliers)

2. **Cochez chaque point :**
   - ✅ Oui = en place, suivi et reconduit
   - ⚠️ Partiel = existe, mais irrégulier / non segmenté / non mesuré
   - ❌ Non = absent

3. **Notez une preuve (si possible) :**
   plan annuel, supports, rapports, résultats, actions correctives.

Exemple

"Tests de restauration mensuels"

- ✅ : test daté et documenté
- ⚠️ : test fait "de temps en temps"
- ❌ : aucun test effectué

Scoring simple

- ✅ = 2 points
- ⚠️ = 1 point
- ❌ = 0 point

Les 5 preuves attendues

1. Plan de sensibilisation (annuel ou trimestriel) + calendrier
2. Segmentation des publics (au moins les fonctions sensibles et nouveaux arrivants)
3. Indicateurs (participation, progression, taux de signalement, résultats de simulation)
4. Simulations / exercices (phishing ou scénarios équivalents) et analyse des résultats
5. Amélioration continue : actions correctives (coaching ciblé, rappels, nouvelles campagnes)

Ce qui compte : La sensibilisation est efficace lorsqu'elle modifie des comportements observables : signalement, vigilance, réduction des erreurs à risque, et qu'elle le démontre.

Vytalx

Périmètre du programme

Un programme efficace n'est pas "un message pour tous".
Il cible les populations à risque, répète les messages essentiels, et mesure l'évolution des comportements.

Populations à couvrir

☐ **Tous les collaborateurs** (socle commun)
☐ **Nouveaux arrivants** (onboarding obligatoire)
☐ **Fonctions sensibles** (Finance, ADV, Direction, Achats, RH)
☐ **IT / Administrateurs** (privilèges, outils, accès)
☐ **Équipes terrain / sites distants** (contraintes, mobilité)
☐ **Prestataires** (si accès SI ou données sensibles)

Thèmes prioritaires

☐ **Phishing / BEC** (fraude au virement, usurpation)
☐ **Mots de passe & MFA** (bonnes pratiques, fatigue MFA)
☐ **Partage de données** (liens, pièces jointes, cloud perso)
☐ **Shadow IT** (outils non approuvés)
☐ **Postes & mobilité** (verrouillage, Wi-Fi, supports amovibles)
☐ **Signalement d'incident** (qui prévenir, comment, quand)
☐ **Règles de base** (mise à jour, macros, téléchargements)

Canaux & cadence

- **Population**
- **Canal** (email, Teams, micro-learning, atelier, affichage...)
- **Cadence** (mensuel / trimestriel / onboarding)
- **Responsable**
- **Indicateur** (participation, score, signalement)

Signaux de risque immédiat :

- Sensibilisation uniquement annuelle et non ciblée
- Aucune mesure (pas d'indicateurs, pas de reporting)
- Pas de parcours nouveaux arrivants
- Populations sensibles non traitées (Finance/Direction)
- Aucun entraînement au signalement (réflexe absent)

Vytalx

Checklist : Gouvernance & programme

Point de contrôle	Oui ✅	Partielle ⚠️	Non ❌	N/A	Preuve ? (oui/non) rapport / capture / procédure / ticket / test daté
Un propriétaire du programme est nommé (pilotage, arbitrage, continuité)	☐	☐	☐	☐	
Objectifs clairs et mesurables (ex. taux de signalement, baisse des clics, ...)	☐	☐	☐	☐	
Plan de sensibilisation formalisé (annuel ou trimestriel)	☐	☐	☐	☐	
Segmentation des publics (au minimum : nouveaux arrivants + fonctions sensibles)	☐	☐	☐	☐	
Cadence définie (récurrence : mensuel/trimestriel + onboarding)	☐	☐	☐	☐	
Intégration à l'onboarding RH (module obligatoire + suivi)	☐	☐	☐	☐	
Messages adaptés au contexte métier (Finance, ADV, Direction, terrain)	☐	☐	☐	☐	
Règles de communication interne (ton, formats, relais managérial)	☐	☐	☐	☐	
Processus de suivi et relance (non complétions, rappels, escalade)	☐	☐	☐	☐	
Gestion des prestataires (si concernés : sensibilisation minimale, règles d'accès)	☐	☐	☐	☐	
Budget/temps alloué (même minimal) et charge d'exploitation cadrée	☐	☐	☐	☐	
Revue périodique du programme (mensuelle/trimestrielle) avec décisions	☐	☐	☐	☐	

Point clé : Un programme de sensibilisation n'est pas un événement : c'est un dispositif récurrent, piloté, et intégré aux parcours (onboarding, populations sensibles, rappels)

Vytalx

Checklist : Contenus & campagnes

Point de contrôle	Oui ✅	Partielle ⚠️	Non ❌	N/A	Preuve ? (oui/non) rapport / capture / procédure / ticket / test daté
Bibliothèque de contenus disponible (socle + modules avancés)	☐	☐	☐	☐	
Formats courts privilégiés (micro-learning, messages simples, répétition)	☐	☐	☐	☐	
Parcours nouveaux arrivants prêt (socle obligatoire : phishing, MFA, signalement)	☐	☐	☐	☐	
Campagnes planifiées (thèmes, calendrier, objectifs)	☐	☐	☐	☐	
Contenus contextualisés métier (finance/BEC, RH, direction, terrain)	☐	☐	☐	☐	
Rappels réguliers “hygiène” (mots de passe, MFA, partage, verrouillage)	☐	☐	☐	☐	
Signalement simplifié et promu (bouton/alias, consignes “1 minute”)	☐	☐	☐	☐	
Kit managers / relais (messages prêts à relayer, affiches, bannières)	☐	☐	☐	☐	
Cohérence avec vos règles internes (chartes, politiques, outils autorisés)	☐	☐	☐	☐	
Sujets “risque immédiat” couverts (phishing/BEC, pièces jointes, liens, macros)	☐	☐	☐	☐	
Sujets “data” couverts (partage externe, cloud perso, confidentialité)	☐	☐	☐	☐	
Canaux adaptés au terrain (affichage, QR codes, sessions courtes)	☐	☐	☐	☐	
Accessibilité & langue (FR, compréhension, formats simples)	☐	☐	☐	☐	

Erreur fréquente : Se limiter à un module annuel générique : le risque humain se traite par répétition, ciblage, et mesure. Pas par un message unique.

Vytalx

Checklist :
Mesure, simulations & amélioration

Point de contrôle	Oui ✅	Partielle ⚠️	Non ❌	N/A	Preuve ? (oui/non) rapport / capture / procédure / ticket / test daté
Indicateurs définis (participation, progression, signalement, résultats)	☐	☐	☐	☐	
Suivi de la participation (par population) avec relances	☐	☐	☐	☐	
Mesure de progression (quiz, score, validation de module)	☐	☐	☐	☐	
Simulations de phishing (ou exercices équivalents) planifiées	☐	☐	☐	☐	
Résultats de simulation analysés (par population, par thème)	☐	☐	☐	☐	
Coaching ciblé pour populations à risque (finance, VIP, récidivistes)	☐	☐	☐	☐	
Mesure du signalement (taux, délai, qualité) et encouragement.	☐	☐	☐	☐	
Boucle d'amélioration continue (actions correctives après campagne)	☐	☐	☐	☐	
Lien avec incidents réels (adapter les contenus aux incidents observés)	☐	☐	☐	☐	
Rituel de revue (mensuel/trimestriel) avec décisions	☐	☐	☐	☐	
Preuves conservées (exports, rapports, comptes rendus) pour audit interne	☐	☐	☐	☐	
Communication de résultats (synthèse à la direction / managers)	☐	☐	☐	☐	

Ce qui prouve l'efficacité : Une sensibilisation utile se voit:
plus de signalement, moins d'erreurs répétées,
et une progression mesurée par population.

Vytalx

Synthèse & plan d'action

Votre résultat

Score total : ____ / ____

Niveau : ☐ Risque élevé (0%-49%) ☐ À consolider (50%-74%) ☐ Structuré (75%-100%)

Barème :	Calcul :
✅ Oui = 2 pts ⚠️ Partiel = 1 pt ❌ Non = 0 pt	**Score obtenu** = somme des points **Score Max** = 2 × (nb de lignes évaluées)

Zones rouges

Vos 5 écarts prioritaires :

_____

_____

_____

_____

_____

Points bloquants

☐ Pas de programme récurrent (sensibilisation "one-shot")
☐ Pas de segmentation (fonctions sensibles, nouveaux arrivants)
☐ Pas d'indicateurs ni de reporting
☐ Pas de simulations / exercices (ou aucun retour analysé)
☐ Pas de boucle d'amélioration (pas d'actions correctives)

Plan d'action

Phase 1 : Cadrage

- Nommer un propriétaire et définir 3-5 objectifs mesurables
- Segmenter : nouveaux arrivants et fonctions sensibles en priorité
- Construire un plan simple (cadence, canaux, relais managers)

Phase 2 : Contenus & canaux

- Mettre en place un socle (phishing/BEC, MFA, partage, signalement)
- Préparer le parcours onboarding (obligatoire et suivi)
- Déployer un canal de signalement clair

Phase 3 : Première campagne

- Lancer une campagne courte (micro-contenus et rappel)
- Préparer une simulation (ou exercice léger)
- Prévoir un kit managers pour relayer

Phase 4 : Mesure & amélioration

- Publier un reporting (participation, résultats, signalement)
- Mettre en place le coaching ciblé (populations à risque)
- Acter les actions correctives et planifier la revue suivante

Mettre en place une sensibilisation continue, pilotée par indicateurs

Une approche industrialisée : sensibilisation continue, simulations et reporting activés selon votre périmètre et vos priorités. L'objectif : obtenir une progression mesurable, concentrer l'effort sur les populations les plus exposées, et disposer de preuves exploitables sans multiplier les outils.

contact/vytalx.fr contact@vytalx.fr