bluesecure

PRÉCONISATIONS D'USAGE

Construire votre programme de sensibilisation à la cybersécurité

Comment structurer votre programme, sur quels indicateurs vous piloter, et comment obtenir les meilleurs résultats.

Document confidentiel. Usage restreint au destinataire @Bluesecure2026

Aucun numéro trouvé

bluesecure

Les 9 questions à se poser pour construire votre plan

Cadrer ces neuf points en amont est le prérequis d'un programme de sensibilisation solide et pilotable.

Pour qui ?

Identification de la population ciblée.

Ex. tout l'effectif, ou une cible prioritaire (comptabilité, RH, nouveaux entrants).

Pourquoi ?

Identification des objectifs généraux.

Ex. réduire le taux de clic phishing, répondre aux exigences ANSSI ou de l'assurance cyber.

Quoi ?

Identification du contenu des messages.

Ex. mots de passe, phishing, IA, CleanDesk, fraude au virement.

Comment ?

Identification des supports de sensibilisation.

Ex. e-learning court, simulations phishing, serious games, quiz.

Quelle communication ?

Identification des supports de communication.

Ex. e-mail de lancement du sponsor, affiches, intranet, newsletter interne.

Quand ?

Identification d'un calendrier prévisionnel.

Ex. un module par mois + une campagne phishing par trimestre sur 12 mois.

Combien ?

Identification d'un budget dédié.

Ex. licences plateforme, temps interne, production de contenu sur-mesure.

Par qui ?

Identification des moyens humains nécessaires.

Ex. sponsor direction, référent RSSI/IT, relais RH et managers.

Quel KPI ?

Identification des indicateurs d'efficacité et de suivi.

Ex. score global, taux de clic ≤ 8 %, compromission ≤ 5 %, complétion ≥ 80 %.

bluesecure

Pourquoi structurer votre sensibilisation

Le facteur humain reste le premier vecteur d'intrusion dans les systèmes d'information. Un programme structuré, régulier et mesuré réduit ce risque de façon concrète , pas seulement pour cocher une case conformité.

Réflexes sécurité

Partager les bonnes pratiques essentielles à l'ensemble de vos collaborateurs.

Prise de conscience

Faire en sorte que chaque métier connaisse les pratiques spécifiques à son exposition.

Responsabilisation

Réduire le facteur humain dans les attaques visant votre système d'information.

bluesecure

Les 3 briques de contenu à combiner

Un programme efficace combine ces trois briques tout au long de l'année — aucune ne remplace les deux autres.

Socle commun

E-learning thématique : mots de passe, phishing, IA, Green IT, CleanDesk, cybercrime… Format court de 10 à 15 min.

Rythme mensuel recommandé

Nouveaux entrants

Parcours d'onboarding cyber dès l'arrivée : e-learning de base, rappel des politiques internes et réflexes essentiels.

En continu toute l'année

Simulations phishing

Campagnes trimestrielles : audit initial, scénarios multiples, puis ciblage par population. Mesure du taux de clic et de signalement.

1 campagne / trimestre minimum

bluesecure

Adapter le rythme à la maturité de vos équipes

Le rythme du socle commun conditionne l'engagement et la mémorisation. Choisissez la cadence adaptée à vos équipes.

OBJECTIF IDÉAL

Mensuel

Un module court chaque mois : c'est ce qui maintient le meilleur niveau d'engagement et de mémorisation.

SEUIL PLANCHER

Bimestriel

Tous les 2 mois, à réserver aux populations qui ont besoin de plus de temps. En dessous, l'effet de répétition se perd.

À retenir : Mensuel = objectif idéal. Bimestriel = seuil plancher, réservé aux populations qui ont besoin de plus de temps pour s'approprier la démarche.

bluesecure

Votre feuille de route sur 12 mois

Exemple de trame pour votre première année à adapter à votre calendrier interne.

	T1	T2	T3	T4
Nouveaux entrants	E-learning + phishing d'accueil, en continu tout au long de l'année			
Socle commun E-learning	Mot de passe · Phishing Email	Phishing IA · CleanDesk	Green IT · Serious Games	Arnaques
Phishing	Audit initial	Multi-scénarios (×5)	Ciblage par population	Bilan annuel & plan N+1

bluesecure

Au-delà de la première année

Une fois les fondamentaux acquis, les campagnes phishing peuvent gagner en réalisme.

Spear phishing ciblé

Ex. un scénario de fraude au virement visant spécifiquement le service comptabilité / paie.

Domaines personnalisés

Scénarios avec un nom de domaine proche du vôtre (typosquatting) pour tester la vigilance.

Usurpation d'identité interne

Un membre de la direction comme expéditeur simulé, pour tester les réflexes face à l'autorité.

Diversifiez les canaux d'attaque simulés

Le phishing ne se limite plus à l'e-mail : testez aussi le **SMS (smishing)**, les **QR codes (quishing)**, les **clés USB piégées** et les **deepfakes** audio / vidéo.

L'objectif n'est pas de piéger vos équipes, mais de **tester leur résistance dans des conditions proches de la réalité** et de mesurer les progrès d'une vague à l'autre.

bluesecure

Cibler l'effort par population

Exemple illustratif — à remplacer par vos propres données une fois votre audit initial réalisé.

POPULATION	TAUX DE CLIC	TAUX DE SIGNALEMENT
Commercial	38 %	4 %
RH	34 %	6 %
Finance	27 %	9 %
Direction	24 %	11 %
Production	18 %	14 %
IT	9 %	22 %

Les populations les plus exposées aux e-mails externes , souvent **commercial, RH** , **achat**, ou encore **COMEX** concentrent le risque : priorisez-les sur vos premières vagues ciblées.

Les populations qui signalent le mieux peuvent devenir des **relais internes** pour entraîner les autres.

Objectif indicatif : réduire l'écart entre vos populations les plus et les moins exposées.

bluesecure

Lancer la démarche en interne

Portée par votre direction ou votre communication interne plutôt que par le seul service IT/sécurité, la légitimité perçue par vos collaborateurs en est renforcée. Voici ce que votre communication doit expliquer.

01

Le contexte

Pourquoi cette démarche, quels risques elle adresse : exemples d'attaques récentes, chiffres du secteur.

02

Les objectifs

Ce que le programme cherche à améliorer, et pour qui.

03

Fréquence & durée

À quoi s'attendre, module par module.

04

Le soutien direction

Un sponsor visible facilite l'adoption du programme.

05

Le bénéfice individuel

Protection des données personnelles, montée en compétence, réflexes utiles hors du travail.

Ces recommandations s'appuient sur les bonnes pratiques promues par l'**ANSSI**. Elles ne remplacent pas une analyse de vos propres obligations réglementaires, à faire valider par votre référent conformité.

bluesecure

Mettre en place un signalement efficace

Sans canal de signalement clair, un programme perd une grande partie de son intérêt : le signalement est **l'indicateur comportemental le plus actionnable**.

Politiques claires
Des directives explicites sur la conduite à tenir face à un e-mail suspect.

Canaux accessibles
Un moyen simple de signaler : bouton, e-mail, téléphone, ticketing.

Anonymat garanti
Une politique de non-répréhension, y compris après un clic sur un scénario simulé.

Réponse rapide
Un processus de traitement déjà prêt en cas d'alerte réelle.

Feedback régulier
Des retours aux personnes qui signalent, pour entretenir la confiance dans le dispositif.

bluesecure

Les KPI à suivre pour piloter votre programme

Des objectifs indicatifs à ajuster selon votre point de départ.

Score global sécurité

≥ 7/10

Niveau de maturité global de vos équipes.

Taux de clic phishing

≤ 10 %

Part des destinataires ayant cliqué sur un scénario simulé.

Taux de compromission

≤ 5 %

Identifiants réellement saisis — le KPI le plus parlant sur le risque réel.

Complétion e-learning

≥ 80 %

Part des collaborateurs ayant terminé les modules assignés.

Taux de signalement

≥ 15 %

Part ayant signalé le scénario au lieu d'y cliquer.

Campagnes / trimestre

≥ 3

Régularité de votre programme dans le temps.

Le KPI à privilégier dans vos comptes-rendus : le taux de compromission plutôt que le seul taux de clic. Il distingue la curiosité sans risque du vrai danger et c'est l'indicateur qui parle le mieux à votre direction.

bluesecure

Bonnes pratiques vs erreurs à éviter

À faire

- Impliquer un sponsor direction dès le lancement
- Répéter les messages sous des formats courts et variés
- Adapter le contenu par métier et niveau d'exposition
- Valoriser publiquement les bons réflexes
- Mesurer et communiquer les progrès régulièrement
- Rendre les sensibilisations obligatoires
- Maximiser les temps forts : Cybermois, journée de la cyber…
- Multiplier les canaux : SMS, QR code, clés USB
- Gamifier au maximum l'expérience d'apprentissage

À éviter

- Une session isolée, sans répétition dans l'année
- Un discours culpabilisant après un clic simulé
- Un contenu unique pour toutes les populations
- Des campagnes déconnectées de l'actualité des menaces
- L'absence d'indicateur de suivi dans le temps

bluesecure

Les facteurs clés de succès

01
Sponsor direction visible et engagé

02
Répétition et régularité des messages

03
Personnalisation par population et métier

04
Ton positif, valorisant, non punitif

05
Canaux de signalement simples et connus

06
Mesure continue et ajustement du plan

Un plan de sensibilisation réussi est **un plan vivant** : il se mesure, s'ajuste et se répète. Il ne se lance pas une fois pour être oublié.

bluesecure

Merci

Nous restons à vos côtés pour configurer, lancer et piloter votre programme de sensibilisation.

contact@bluesecure.io