bluesecure

KIT DE COMMUNICATION - À L'USAGE DES CLIENTS & PARTENAIRES

Communiquer sur Bluesecure auprès de vos utilisateurs

Messages clés, éléments de langage et modèles prêts à l'emploi pour présenter la sensibilisation cyber à vos collaborateurs.

Document public · contact@bluesecure.fr

BIENVENUE

Un kit pensé pour vous faire gagner du temps

Ce guide a été conçu pour vous aider à valoriser vos campagnes de sensibilisation et à renforcer l'engagement de vos collaborateurs autour de la cybersécurité. Vous y trouverez des messages clés, des éléments de langage et des modèles prêts à l'emploi.

Notre objectif : vous permettre d'adapter facilement chaque support à votre identité et à vos besoins de communication, tout en conservant un discours clair, cohérent et rassurant.

Ce que contient ce guide

01 À propos de BlueSecure

02 Pourquoi sensibiliser

03 Présenter BlueSecure (le pitch)

04 Messages clés par audience

05 Les cybergames™ (serious games)

06 Animer votre campagne

07 La newsletter cyber mensuelle

08 Le bouton de signalement

09 Modèles d'emails

10 Do & Don't de communication

11 Kit visuel & identité

A Annexe — Guide collaborateur (utilisateurs finaux)

i

Comment utiliser ce guide

Piochez les sections utiles à votre contexte. Les blocs surlignés en violet sont des **textes à copier-coller** et à personnaliser (nom de l'entreprise, dates, contact interne).

01 À PROPOS

Qui est Bluesecure ?

Bluesecure est un cabinet d'audit et de conseil en cybersécurité. Nous aidons les organisations à renforcer leur posture de sécurité face aux menaces d'ingénierie sociale, grâce à une plateforme de sensibilisation aux risques cyber.

La plateforme , **certifiée Qualiopi et référencée DataDock,** propose des formations en ligne et en présentiel sur la cybersécurité, la réglementation et la protection des données, ainsi que des campagnes de phishing simulées : e-mails, SMS, clés USB, réseaux sociaux et appels téléphoniques.

100%

Société française, basée à Paris (Bluedigital SAS)

Qualiopi

Certifié qualité & référencé DataDock

5 canaux

Phishing simulé : e-mail, SMS, USB, réseaux sociaux, téléphone

Notre approche

Nous rendons la cybersécurité **accessible** grâce à la gamification de l'apprentissage. Plutôt que de culpabiliser les utilisateurs, nous les impliquons activement : chaque collaborateur devient un maillon fort de la sécurité de l'organisation.

02 LE CONTEXTE

Pourquoi sensibiliser vos collaborateurs

La grande majorité des incidents de sécurité impliquent un facteur humain. Un email piégé, un mot de passe réutilisé, une pièce jointe ouverte trop vite : les attaquants ciblent d'abord les personnes. Sensibiliser, c'est transformer ce risque en première ligne de défense.

Réduire les risques cyber

Des collaborateurs formés détectent mieux les tentatives d'hameçonnage et adoptent les bons réflexes au quotidien.

Répondre à vos obligations

La sensibilisation contribue à la conformité (RGPD, exigences assurantielles, référentiels de sécurité).

Créer une culture commune

La sécurité devient l'affaire de tous, portée positivement plutôt que subie.

Protéger l'organisation

Moins d'incidents, c'est protéger les données, la réputation et la continuité de l'activité.

L'IDÉE CLÉ À FAIRE PASSER

« La cybersécurité n'est pas qu'une affaire d'experts. Chacun, à son poste, peut faire la différence. »

03 LE PITCH

Présenter Bluesecure à vos utilisateurs

Selon le temps dont vous disposez, adaptez la longueur de votre présentation. Voici trois formats prêts à l'emploi.

EN UNE PHRASE

« Nous déployons Bluesecure, une plateforme de sensibilisation à la cybersécurité qui nous aide, tous, à reconnaître les tentatives d'arnaque et à adopter les bons réflexes. »

ARGUMENTAIRE ORAL · 30 SECONDES

« Les cyberattaques visent d'abord les personnes : un email piégé, un faux SMS, un appel qui semble légitime. Pour nous aider à les repérer, nous mettons en place BlueSecure. C'est une plateforme simple, en ligne, avec de courts modules et des mises en situation concrètes. L'objectif n'est pas de nous piéger, mais de nous entraîner pour protéger nos données, nos clients et notre entreprise. Cela ne prend que quelques minutes, et chacun avance à son rythme. »

VERSION COMPLÈTE · 3 POINTS

1. **Le pourquoi.** Les menaces ciblent le facteur humain. Nous voulons protéger l'entreprise et chaque collaborateur.
2. **Le comment.** Des modules courts en ligne, des mises en situation réalistes, une progression à votre rythme.
3. **Le bénéfice.** Des réflexes utiles au bureau comme à la maison. Une démarche positive, sans jugement.

04 MESSAGES CLÉS

Adaptez le message à votre audience

Le même dispositif ne se raconte pas de la même façon à la direction, aux managers et aux collaborateurs. Voici l'angle à privilégier pour chaque public.

Direction & comité exécutif

Angle : maîtrise du risque et conformité.

« Réduire notre exposition aux cyberattaques, répondre à nos obligations réglementaires et protéger la continuité de notre activité. »

Managers & relais internes

Angle : accompagnement de l'équipe et exemplarité.

« Encouragez votre équipe à suivre les modules. Votre implication donne le ton : la démarche est positive et sans jugement. »

Collaborateurs (utilisateurs finaux)

Angle : simplicité, utilité concrète, bénéfice personnel.

« Quelques minutes pour apprendre à déjouer les arnaques ,des réflexes utiles au travail comme à la maison. Vous avancez à votre rythme. »

05 SERIOUS GAMES

Engagez vos équipes avec nos cybergames™ primés

Des serious games interactifs et immersifs, disponibles en ligne ou sur site avec un animateur. Un excellent levier pour animer une journée de sensibilisation et marquer les esprits bien au-delà des modules e-learning.

Lauréat Or · Cybernight 2024 · 45 min

Cybercrime™

9 pièces, 6 armes, 6 suspects et 9 mini-jeux pour débloquer des indices. Des scénarios réalistes qui plongent les participants dans des énigmes de cybersécurité pour développer les bons réflexes.

Pour les développeurs · 30 min

Red code™

Un escape game cyber pensé pour les équipes techniques. À travers une enquête interactive avec vidéos et écrans simulés, identifiez la faille et choisissez le bon correctif parmi plusieurs propositions.

Immersif 45 min

BlueScreen™

L'utilisateur se glisse dans la peau d'un pirate qui prépare une cyberattaque contre un hôpital. À chaque défi, il est confronté à plusieurs choix.

Nouveau Coup de cœur Jury 2025

30 min

Blackout™

Un escape game immersif de gestion de crise : incarnez tour à tour les acteurs clés (pilote de crise, DPO, COMEX, support informatique, communication) et prenez les bonnes décisions sous pression pour limiter l'impact. Accessible à tous les profils.

Idée Associez un cybergame à votre lancement de campagne ou à un temps fort (mois de la cybersécurité) pour créer un moment fédérateur. Pour organiser une session, contactez votre interlocuteur BlueSecure ou écrivez à **contact@bluesecure.fr**.

06 DISPOSITIFS D'ANIMATION

Faire vivre votre campagne

Au-delà des modules, Bluesecure met à disposition des supports pour rythmer votre campagne, entretenir l'attention et ancrer les bons réflexes dans la durée.

Événements & journées de sensibilisation

Des temps forts en présentiel, animés par un intervenant BlueSecure : cybergames, ateliers et démonstrations. Idéal pour lancer une campagne ou marquer le mois de la cybersécurité.

Teaser vidéos

De courtes vidéos à diffuser en interne (intranet, écrans, réunions) pour annoncer la campagne et susciter la curiosité avant le lancement.

Signatures d'e-mail personnalisées

Des bannières de signature aux couleurs de la campagne, à déployer sur les messageries pour rappeler la démarche à chaque échange.

Goodies & kits physiques

Des supports tangibles (affiches, stickers, objets) pour prolonger le message sur le lieu de travail et entretenir la mémoire des bons réflexes.

Bon à savoir Ces supports sont disponibles auprès de votre interlocuteur Bluesecure. Prévoyez-les en amont pour aligner le calendrier de diffusion avec le lancement de vos modules.

07 CONTENU RÉCURRENT

La newsletter cyber mensuelle

Chaque mois, les administrateurs Bluesecure reçoivent une newsletter dédiée à l'actualité cyber, avec notamment des **cas d'attaques réelles** décryptés. Un moyen simple d'entretenir la vigilance entre deux campagnes.

Pour vous, administrateurs

L'actualité Bluesecure et une veille prête à l'emploi : tendances, menaces du moment et cas concrets, pour rester informé sans effort de recherche.

Une partie dédiée aux utilisateurs

En fin de newsletter, un contenu pensé pour vos collaborateurs, que vous pouvez **transférer tel quel** ou dont vous pouvez **réutiliser le texte** dans vos propres supports.

Comment l'utiliser

1. À réception, repérez la section « utilisateurs » en bas de la newsletter.
2. Transférez-la à vos équipes, ou intégrez le cas d'attaque du mois à votre communication interne (intranet, canal Teams/Slack).
3. Adaptez éventuellement le ton et ajoutez un mot de contexte propre à votre organisation.

08 RÉFLEXE CLÉ

Communiquer sur le bouton de signalement

Le bouton de signalement s'intègre à la messagerie de vos collaborateurs et leur permet de signaler un e-mail suspect **en un seul clic**. C'est le geste le plus utile au quotidien ,encore faut-il en parler pour créer le réflexe.

Simple

Un clic depuis l'e-mail suspect suffit. Pas besoin de rédiger un rapport ni de transférer manuellement.

Utile

Chaque signalement aide à protéger toute l'organisation et à réagir plus vite face à une menace.

Sans risque

Mieux vaut un signalement de trop qu'un incident : signaler par précaution n'est jamais une erreur.

Le message à faire passer

« Un e-mail vous semble étrange ? Ne cliquez pas, ne répondez pas : signalez-le en un clic grâce au bouton de signalement. C'est simple, rapide, et cela protège tout le monde. Dans le doute, signalez. »

Astuce Le bouton est déployé sur les messageries par votre service informatique. Rappelez régulièrement son existence en signature, en réunion d'équipe, ou après une campagne de phishing simulé pour transformer le geste en réflexe.

09 MODÈLES

Email d'annonce de lancement

Copiez-collez ce modèle et remplacez les champs entre crochets. Envoyez-le idéalement quelques jours avant le démarrage de la campagne.

Objet : Nouvelle démarche cybersécurité — quelques minutes pour vous protéger
De : [Direction / RSSI / RH] · À : Tous les collaborateurs

Bonjour à toutes et à tous,

Les cyberattaques sont de plus en plus fréquentes, et elles visent d'abord les personnes : emails piégés, faux SMS, appels frauduleux. Pour nous aider à les reconnaître et à adopter les bons réflexes, **[Nom de l'entreprise]** met en place **Bluesecure**, une plateforme de sensibilisation à la cybersécurité.

Concrètement, vous suivrez de **courts modules en ligne** et des mises en situation réalistes. L'objectif n'est pas de vous piéger, mais de vous entraîner, à votre rythme. Cela ne prend que quelques minutes, et les réflexes acquis vous serviront aussi dans votre vie personnelle.

Vous recevrez prochainement un accès à la plateforme, à partir du **[date de lancement]**. En cas de question, vous pouvez contacter **[référent interne / email]**.

Merci d'avance pour votre implication : ensemble, nous renforçons la sécurité de **[Nom de l'entreprise]**.

Bien à vous,
[Signature]

Astuce Personnalisez le ton selon votre culture d'entreprise. Une relance courte quelques jours après le lancement augmente sensiblement le taux de participation.

10 BONNES PRATIQUES

Do & Don't de communication

Quelques repères simples pour un message qui engage plutôt qu'il n'inquiète.

À faire

- Adopter un ton positif et bienveillant
- Mettre en avant le bénéfice concret
- Rappeler que la démarche est un entraînement, pas un contrôle
- Impliquer les managers comme relais
- Rester simple, éviter le jargon technique
- Valoriser les progrès collectifs

À éviter

- Culpabiliser ou pointer les erreurs individuelles
- Employer un ton anxiogène ou menaçant
- Présenter cela comme une surveillance
- Multiplier le jargon et les sigles
- Nommer publiquement les personnes « piégées »
- Sur-solliciter par des rappels trop fréquents

Le ton Bluesecure en un mot

Professionnel, direct et rassurant. Des phrases courtes, des verbes à l'action, le bénéfice avant la fonctionnalité. La cybersécurité est rendue **accessible** , jamais anxiogène.

Kit visuel & usage du logo

Le logo BlueSecure est un élément essentiel de notre image de marque. Merci de respecter ces consignes avant toute utilisation.

bluesecure

Sur fond clair - version couleur

bluesecure

Sur fond foncé - version claire

À respecter

- Préserver les marges de sécurité autour du logo
- Utiliser la bonne variante selon le fond
- Conserver les proportions d'origine

À ne pas faire

- Modifier les couleurs, la police ou la structure
- Déformer, étirer ou pivoter le logo
- Le placer sur un fond peu contrasté

Couleurs de marque

#4650D0 #2F37A0 #CDBBF7 #14162B

Typographie

Aa

Titres - Inter

Aa

Corps - Inter

ANNEXE · À DIFFUSER AUX UTILISATEURS FINAUX

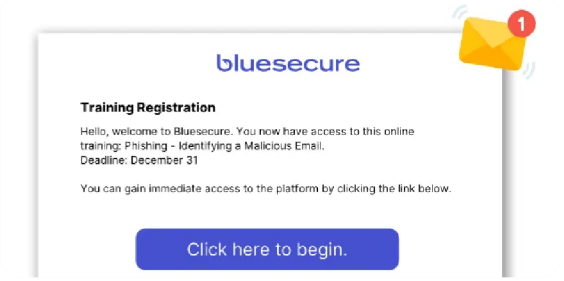
Guide collaborateur

Accéder à la plateforme, suivre vos formations et valider vos acquis, en quelques étapes simples.

1 Connectez-vous à l'interface

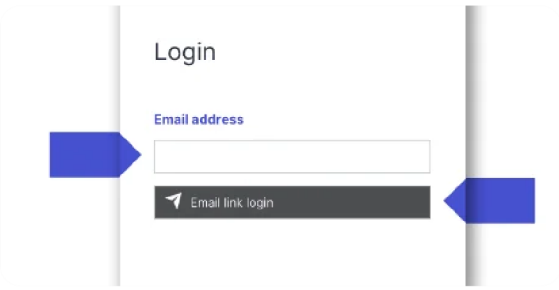
Option 1 - Invitation par e-mail

Vérifiez vos e-mails et trouvez l'invitation envoyée depuis **noreply@bluesecure.io**. Cliquez ensuite sur le bouton « Cliquez ici pour commencer ».



Option 2 - Lien de connexion

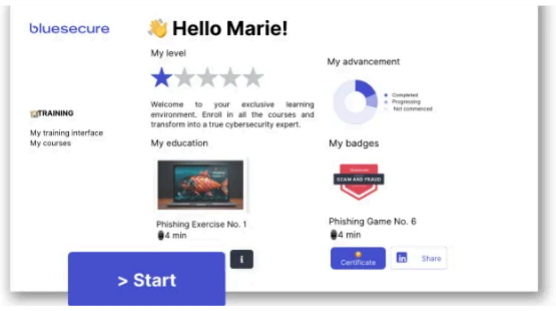
Sur la page de connexion, saisissez votre adresse e-mail et cliquez sur « Se connecter avec un lien par email ». Un message de **noreply@bluesecure.io** vous permettra d'accéder à l'interface.



Astuce Pensez à ajouter ce lien à vos favoris pour le retrouver facilement.

2 Accédez à vos formations

Une fois sur l'interface, cliquez sur **« Mes formations »** puis sur **« Commencer »** pour suivre la formation en ligne. Pour reprendre une formation déjà entamée, cliquez sur **« Continuer »** , vous repartez du point où vous vous êtes arrêté.

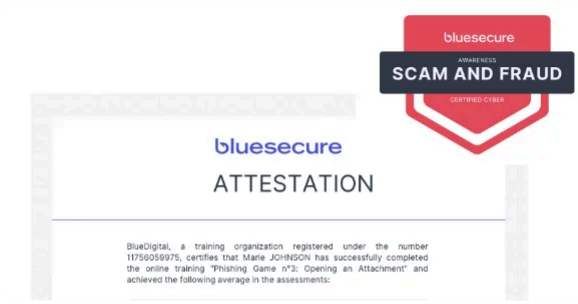


3 Téléchargez votre fiche mémo

Pour certaines formations, vous pouvez télécharger une **fiche mémo au format PDF** : un résumé pratique des points clés à conserver et à consulter au besoin.

4 Validez vos acquis avec un quiz

Après la formation, si un quiz est disponible, participez-y et découvrez le corrigé juste après. À partir de **80 % de bonnes réponses**, le module est validé. Vous pouvez alors télécharger votre **certificat de réussite** depuis votre tableau de bord, via l'option « Certificat ».



ANNEXE · GUIDE COLLABORATEUR

Le bouton de signalement

À quoi sert ce bouton ?

En un clic, il vous permet de **signaler un message suspect** au support informatique / à l'équipe sécurité, afin de :

- **Protéger plus vite** l'organisation (détection et traitement accélérés)
- **Centraliser** les signalements au même endroit
- **Réduire la charge** de tri et d'analyse côté équipes
- Vous donner un **retour immédiat** après votre signalement

Comment ça marche ?

1. **Sélectionnez l'email** qui vous paraît suspect.
2. Cliquez sur **« Signaler avec Bluesecure »** (barre d'outils ou menu des options de votre messagerie).
3. **Confirmez** l'envoi du signalement.

C'est tout. Inutile de transférer l'email à des collègues ou de multiplier les actions.

Après le signalement

Vous recevez un **accusé de réception immédiat**. Selon la configuration retenue par votre organisation :

- Une **analyse automatique** peut estimer le niveau de suspicion (si activée).
- Si l'email faisait partie d'une **simulation**, vous recevez un message de confirmation.
- Si l'email est **réel**, vous recevez une confirmation de prise en charge : il est transmis aux équipes pour investigation.

Les bons réflexes

- ✓ **Signalez** dès que vous avez un doute, même sans être sûr à 100 %.
- ✗ Ne cliquez pas sur un lien et n'ouvrez pas une pièce jointe suspecte.
- ✗ Ne répondez pas au message et ne le transférez pas « pour avis » à des collègues.

Déjà cliqué ?

Si vous avez déjà cliqué ou saisi un mot de passe, **contactez immédiatement le support informatique** via vos canaux habituels : **[à compléter : téléphone / portail support / Teams]**.

Où trouver le bouton ?

Le bouton apparaît sous l'intitulé **« Signaler avec Bluesecure »** dans votre messagerie, une fois le déploiement effectué sur votre compte par votre service informatique.

ANNEXE · GUIDE COLLABORATEUR

Questions fréquentes des utilisateurs

Qu'est-ce que Bluesecure ?

BlueSecure est une entreprise française accréditée (n° d'enregistrement 11756059975) et certifiée Qualiopi. Elle propose des programmes de sensibilisation à l'ingénierie sociale, incluant des simulations de phishing sur divers canaux ainsi qu'une plateforme de formation à la cybersécurité et aux sujets réglementaires.

Est-il obligatoire de suivre les formations ?

Oui. Ces formations sont essentielles pour garantir la conformité et la sécurité de votre organisation.

La formation est-elle certifiante ?

En tant qu'organisme de formation, nous délivrons une attestation prouvant que vous avez suivi la formation et réussi les tests de validation des acquis. Elle est téléchargeable au format PDF, comme preuve de conformité en cas de contrôle. Vous l'obtenez une fois le module terminé, c'est-à-dire après avoir visionné l'ensemble du contenu et validé les quiz avec 80 % de bonnes réponses. Un quiz peut être repassé si ce seuil n'est pas atteint à la première tentative.

Combien de temps la formation reste-t-elle disponible ?

Vous pouvez y accéder sans limite de temps et vous reconnecter plus tard pour revoir un point précis. Votre organisation a toutefois pu fixer une date limite pour suivre le module dans ce cas, vous en avez été informé par une communication dédiée.

Combien de temps le lien d'invitation est-il valide ?

Le lien expire 7 jours après l'envoi. En cliquant sur un lien expiré, l'application vous propose de saisir votre adresse e-mail pour recevoir un nouveau lien de connexion valide.

Comment fonctionne le lecteur ?

La barre de progression, affichée en pourcentage, indique votre avancement. Sous le lecteur, le bouton « Navigation » donne accès aux chapitres, et « Sauvegarder et quitter » enregistre votre progression pour reprendre plus tard là où vous vous êtes arrêté.

Comment changer la langue des formations ?

Contactez votre responsable de formation au sein de votre organisation.

Que faire en cas de non-réception de l'invitation ?

Trois options :

- Vérifiez votre dossier « Spam » ou « Courrier indésirable ».
- Rendez-vous sur la page de connexion, saisissez votre adresse e-mail : vous recevrez un lien temporaire de connexion.
- Demandez à votre superviseur de formation de vous renvoyer une invitation.

D'autres questions ?

N'hésitez pas à contacter votre service informatique ou votre service RH.

ASSISTANCE & CONTACT

Besoin d'un format spécifique ou d'un visuel sur mesure ?

Écrivez-nous : un membre de notre équipe vous répondra rapidement et vous accompagnera dans votre communication.

contact@bluesecure.fr

www.bluesecure.fr

bluesecure

BlueDigital SAS - Société par Actions Simplifiée, immatriculée au Registre du Commerce et des Sociétés de Paris sous le numéro 833 999 352, dont le siège social se situe 1 cours Valmy PUTEAUX 92800 Nom commercial : Bluesecure. www.bluesecure.fr