

Janvier 2026

Votre année
2026 avec
bluesecure

2026

Chers clients,

Toute l'équipe de **BlueSecure** vous souhaite une excellente année **2026**, pleine de succès et de cybersécurité renforcée !

Nouveautés de Janvier

1

Nouveau micro-learning:
Comprendre & utiliser le VPN

2

Nouveau micro-learning:
Authentification Multi-Facteurs (MFA)

3

Nouveau micro-learning:
Phishing sur les messageries instantanées

Nouveau micro-learning - Comprendre & utiliser le VPN

Découvrez notre nouveau module consacré au **VPN (Virtual Private Network)**, un outil essentiel pour garantir la sécurité des données lorsque vous travaillez à distance. Ce micro-learning explique de façon simple et concrète **son fonctionnement, ses avantages et les bonnes pratiques d'utilisation**, afin de protéger efficacement les informations de l'entreprise en dehors du bureau.

À travers des exemples du quotidien, ce module vous aidera à **adopter les bons réflexes** : activer le VPN à chaque connexion externe, éviter les réseaux publics non sécurisés et utiliser exclusivement la solution fournie par l'entreprise.



Nouveau micro-learning - Authentification Multi-Facteurs (MFA)

Renforcez la sécurité de vos comptes grâce au MFA, qui combine plusieurs facteurs pour vérifier votre identité. Ce module explique de manière simple **le fonctionnement du MFA**, pourquoi il est essentiel pour se protéger contre les attaques par mot de passe et présente les bonnes pratiques pour l'utiliser efficacement au quotidien. **Chiffre clé : le MFA bloque plus de 99% des attaques par mot de passe**, ce qui en fait un outil indispensable pour sécuriser vos accès professionnels et

personnels.



⚠ Nouveau micro-learning - Phishing sur les messageries instantanées



Les cybercriminels ne se limitent plus aux emails et utilisent désormais **Teams, Slack, WhatsApp, LinkedIn ou Messenger** pour tenter de vous piéger. Ce module vous guide pour identifier les messages suspects, même lorsqu'ils semblent provenir d'un collègue, éviter de cliquer sur des liens douteux ou de télécharger des fichiers piégés et savoir comment signaler immédiatement toute tentative suspecte à votre service informatique.

Mon espace

La cybersécurité ne peut plus se limiter à des outils techniques : elle repose aussi sur des gestes simples du quotidien et une culture de la vigilance partagée.

Restez informé(e), restez protégé(e).

Une question ? N'hésitez pas à contacter votre service informatique.



Cliquez [ici](#) pour consulter les newsletters précédentes. Pour rester informé sur l'actualité cyber et sur les nouveautés BlueSecure, suivez-nous sur les réseaux sociaux.

Cas d'attaque : La Poste frappée par une cyberattaque en plein rush de Noël

Le groupe **La Poste** a été victime d'une **cyberattaque de grande ampleur** qui a rendu **ses services en ligne indisponibles**, perturbant l'accès aux plateformes numériques de suivi de colis, aux applications mobiles et à certains services bancaires de **La Banque Postale**. Selon les autorités et l'opérateur, il s'agit d'un **incident de type déni de service (DDoS)** visant à saturer les serveurs et les rendre inaccessibles, sans pour autant compromettre les données personnelles des utilisateurs jusqu'à présent.

L'attaque, **revendiquée par un groupe de hackers prorusses appelé NoName057**, a ciblé La Poste au moment où l'entreprise traite des **centaines de millions de colis et courriers**, une période particulièrement critique pour la logistique et les services bancaires en ligne. Le parquet de Paris a ouvert une enquête confiée à la *Direction générale de la sécurité intérieure* (DGSI) et à l'*Unité nationale cyber*.

 Les points clés à retenir :

- Une **attaque DDoS majeure** a rendu les sites web, applications et services numériques de La Poste inaccessibles au pic de l'activité de fin d'année.
- **La Banque Postale** a également vu ses services en ligne perturbés, contraignant les utilisateurs à des solutions alternatives comme l'authentification par SMS pour certains paiements.
- L'incident a **perturbé le suivi des colis et l'accès aux services digitaux** sans toutefois interrompre complètement la distribution physique du courrier et des colis.

Un problème technique ?

Veuillez contacter notre support. Pour toutes demandes fonctionnelles, n'hésitez pas à contacter votre **Customer Success Manager** qui vous **assistera** dans l'utilisation de notre solution.

@BlueSecure2026, La Défense, PARIS , FRANCE

[Se désabonner](#) [Gérer les préférences](#)