

Nouveautés **Mai 2026**

bluesecure



1

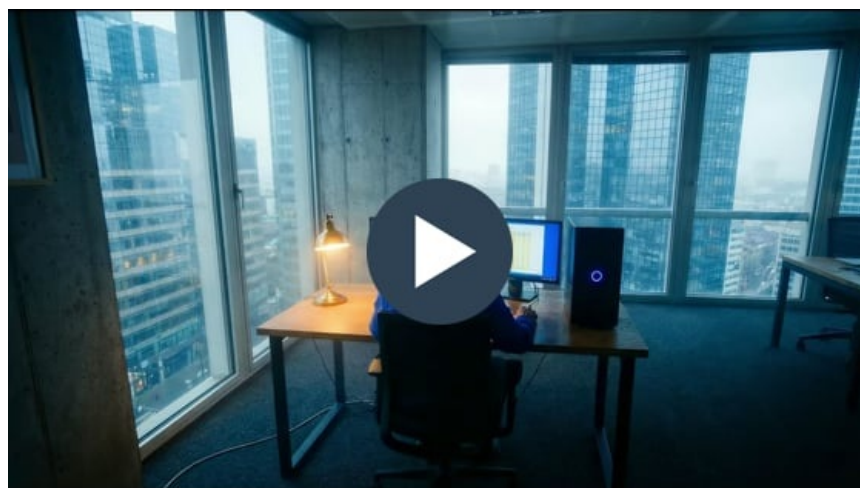
Nouveau module interactif:
Blackout - Gestion de crise

2

Nouveau micro-learning:
**IA Générative : comprendre,
utiliser, sécuriser**

3

Campagne de phishing:
Nouveaux scénarios



Tester BlackOut



Nouveau micro-learning - IA Générative: comprendre, utiliser, sécuriser

Nouveau programme dédié à **l'IA générative**, conçu pour tous les collaborateurs en seulement 30 minutes. À travers **plusieurs modules courts** et complémentaires, vous apprendrez à comprendre ce qu'est réellement l'IA générative et son fonctionnement, à **maîtriser l'art du prompt** pour en tirer des résultats pertinents, et à identifier des cas

d'usage concrets dans votre quotidien professionnel. Le parcours aborde également les autres capacités de l'IA (images, code, analyse), propose des **misés en situation interactives** et met l'accent sur **les limites, les risques et les bonnes pratiques**, notamment en matière de **sécurité des données** ; un format complet pour adopter une **utilisation efficace, responsable et sécurisée de l'IA**.

Créer ma campagne learning

Nouveaux scénarios de phishing

- Notion - Activer votre compte
- Adobe - Signature bon de commande
- Apple - Connexion Suspecte
- Airbnb - Modification de mot de passe
- Amazon - Paiement décliné
- Spendesk - Compte suspendu - Email
- Pipedrive - Réinitialiser votre mot-de-passe - Email

Créer ma campagne phishing

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.



Pour rester informé sur l'actualité cyber et sur les nouveautés BlueSecure, suivez-nous sur les réseaux sociaux.

Cas d'attaque : cyberattaque contre Basic-Fit — près d'un million de membres exposés en Europe

La chaîne de salles de sport **Basic-Fit** a été victime d'une **cyberattaque éclair** ayant entraîné la fuite des données personnelles d'environ **un million de membres à travers l'Europe**. L'attaque, particulièrement rapide, a permis aux cybercriminels d'accéder à des informations sensibles, soulevant des inquiétudes sur la sécurité des plateformes numériques dans le secteur du fitness.

Parmi les données compromises figurent **noms, adresses email, numéros de téléphone et informations liées aux abonnements**.

Bien que les mots de passe et données bancaires ne semblent pas avoir été affectés, cette fuite expose les utilisateurs à des risques accrus de phishing et d'usurpation d'identité. L'incident met en lumière la vulnérabilité des entreprises face à des attaques rapides et ciblées.

Les points clés à retenir :

- Près d'un million de membres touchés dans plusieurs pays européens
- Données personnelles exposées : noms, emails, numéros de téléphone, informations d'abonnement
- Risque élevé de phishing et d'escroqueries ciblées

Rappel des bonnes pratiques :

- Méfiez-vous des e-mails suspects : Vérifiez toujours l'adresse de l'expéditeur et soyez prudent(e) avec les liens et pièces jointes.
- Utilisez des mots de passe complexes: Privilégiez des phrases longues ou des générateurs de mots de passe et activez l'authentification à deux facteurs.
- Mettez vos logiciels à jour régulièrement : Les mises à jour corrigent des failles de sécurité exploitées par les cybercriminels.
- Vérifiez régulièrement vos comptes et dossiers : si vous constatez une activité inhabituelle (changement de données, accès que vous ne reconnaissez pas), signalez-le immédiatement.
- Soyez vigilant face à l'ingénierie sociale : Les hackers jouent sur vos émotions (urgence, peur, curiosité) pour vous inciter à divulguer des informations sensibles.

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](#)