

Novembre 2025

Ne manquez pas les nouveautés du mois de **bluesecure.fr**



Bonjour,

Je suis ravie de vous retrouver pour découvrir **les nouveautés** du **mois de Novembre** !

Au programme ce mois-ci :

1

Nouveau micro-learning :
Comprendre et utiliser un VPN

2

Nouveau micro-learning :
Le cycle de vie de l'information

3

Nouveau micro-learning :
Arnaque à la webcam

Nouveau micro-learning - Comprendre et utiliser un VPN

Renforcez la sécurité du travail à distance avec notre micro-learning dédié au **VPN**, l'outil qui protège vos connexions hors du bureau. En quelques minutes, vos utilisateurs comprennent quand l'activer, pourquoi il est indispensable et les **bons réflexes à adopter** sur les réseaux publics.



Nouveau micro-learning - Le cycle de vie de l'information



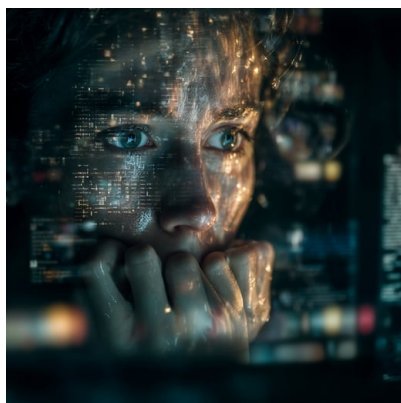
Découvrez notre nouveau micro-learning **“Le cycle de vie de l’information”**, conçu pour aider chaque collaborateur à protéger les données à chaque étape : création, utilisation, partage, archivage et destruction.

En moins de 5 minutes, vos équipes apprennent **les bons réflexes** pour éviter fuites, erreurs et mauvaises pratiques du quotidien.

🛡️ Nouveau micro-learning - Arnaque à la webcam

Un nouveau micro-learning aide vos utilisateurs à reconnaître et déjouer **l’arnaque à la webcam**, un chantage très courant qui joue sur la peur et l’urgence.

En quelques minutes, ils apprennent à identifier ces faux messages, à réagir avec sang-froid et à renforcer la sécurité de leurs mots de passe et équipements.



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.

Cyberattaque Weda : des milliers de cabinets médicaux paralysés et près de 20 000 professionnels touchés

Weda, l'un des principaux logiciels utilisés par les médecins libéraux pour gérer les dossiers patients, a été **victime d'une cyberattaque** dans la nuit du 10 novembre 2025. Une activité anormale a été détectée sur ses serveurs, poussant l'éditeur à **couper immédiatement l'accès à la plateforme** pour protéger les données. Cette décision a **paralysé plus de 20 000 professionnels de santé**, soudain privés d'accès aux antécédents, traitements et documents médicaux de leurs patients. Les cabinets ont dû fonctionner **en mode dégradé**, avec des consultations ralenties et parfois reportées. À ce stade, Weda confirme que des accès malveillants ont pu permettre une extraction partielle de données, mais l'ampleur exacte de la fuite reste encore inconnue.

 Les points clés à retenir :

- Le secteur de la santé est de plus en plus ciblé : selon ANSSI, la part des incidents informatiques dans ce secteur est passée de 2,87 % en 2020 à 11,4 % en 2023.
- Plus de **20 000 professionnels de santé** utilisant Weda sont concernés par l'interruption du service
- Risque accru de **phishing ciblé et usurpation d'identité**

 **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.