

Septembre 2025

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



Bonjour,

Je suis ravie de vous retrouver pour vous présenter les **nouveautés de Septembre !**

1

Retrouvez-nous aux **Assises**

2

Nouveau micro-learning:
La sécurité physique

3

Un nouveau phishing game sur **WhatsApp**



retrouvez-nous aux Assises !

LA 25

08.10.25 →→ 11.10.25

/MONACO///

LES ASSISES

**NOUS SERONS
AU VILLAGE
START-UPS !**

Nous avons hâte
de vous rencontrer !

25
ANS

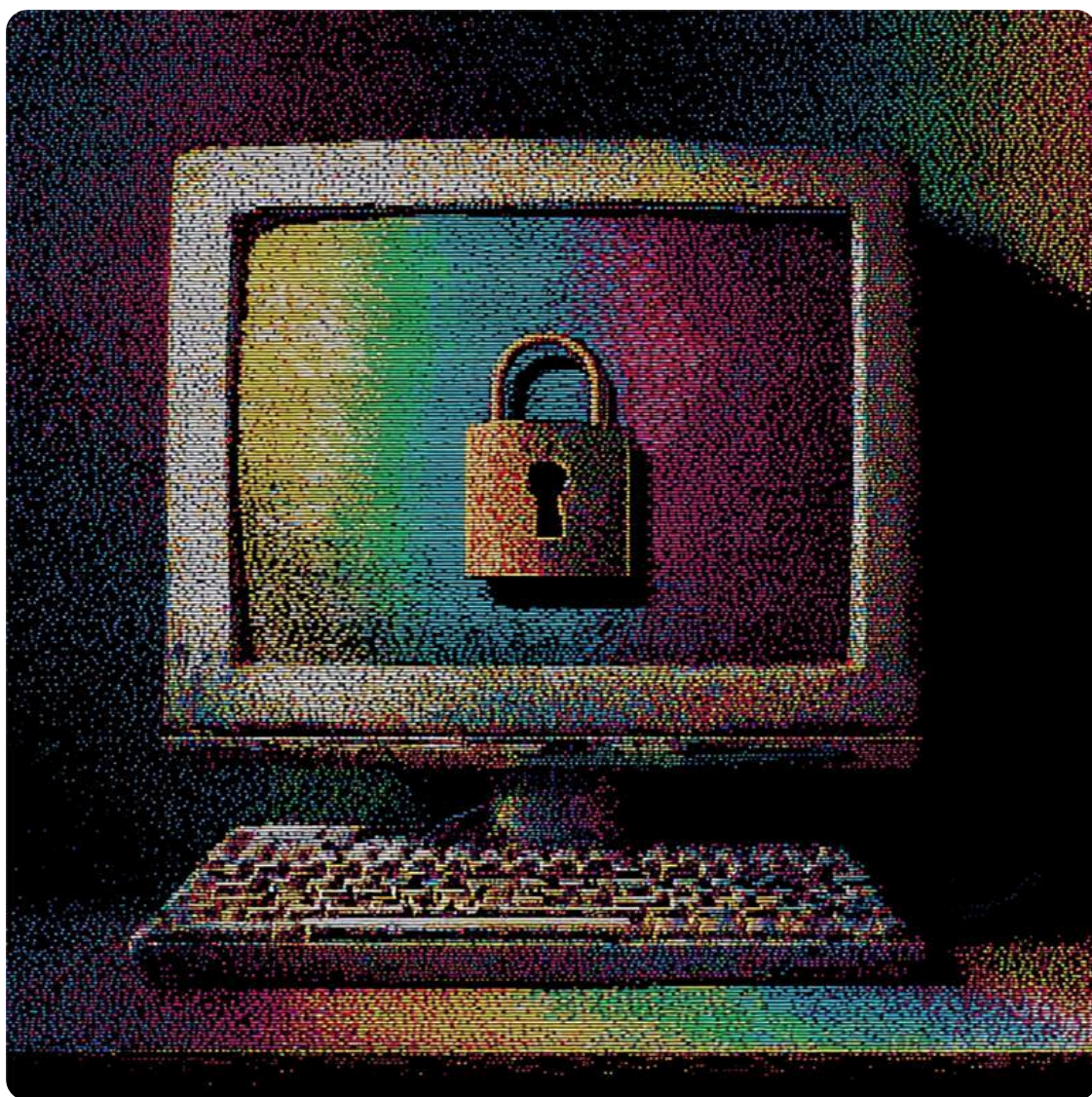
bluesecure

ELEVATOR PITCH ▶ 09/10 - 11H40

lesassisesdelacybersecurite.com

 **Nouveau micro-learning – La sécurité physique**

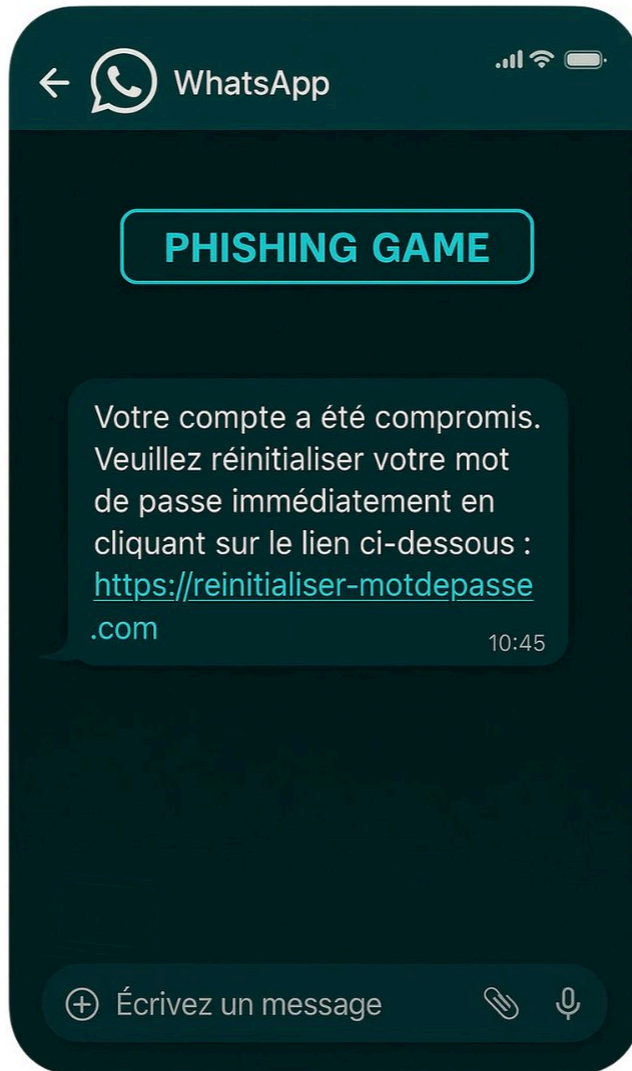
Nous enrichissons notre catalogue de formation avec un nouveau module dédié à **la sécurité physique**. Ce contenu pédagogique de **3 minutes** sensibilise de manière claire et concrète aux risques liés à un manque de vigilance dans les espaces de travail : vol d'équipements, accès non autorisés, espionnage ou encore sabotage. À travers des **misés en situation réalistes** et des conseils pratiques, les collaborateurs découvrent **les bons réflexes** à adopter pour protéger leurs données, leurs équipements et leur environnement professionnel. **Accessible à tous les profils**, ce module permet de renforcer la culture de sécurité sur un aspect souvent négligé, mais essentiel au quotidien.



Un nouveau phishing game sur WhatsApp

Nouveau **Phishing Game dédié à WhatsApp**, à travers une interface reproduisant fidèlement une conversation, vos collaborateurs sont confrontés à plusieurs **scénarios d'arnaques** couramment utilisées par les cybercriminels sur mobile. Le but : identifier les signaux d'alerte, comprendre les mécanismes d'ingénierie sociale

et adopter les bons réflexes face à des messages suspects. Chaque situation est accompagnée d'**explications pédagogiques** pour consolider les apprentissages. Plusieurs scénarios sont disponibles, afin de couvrir un large éventail de techniques d'usurpation et de manipulation.



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, 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: Adecco victime d'un piratage massif - 70 000 victimes, une faille humaine à l'origine

Le groupe Adecco, leader mondial de l'intérim, a été la cible d'un piratage massif ayant compromis les données personnelles de plus de **70 000 personnes**.

À l'origine de l'attaque : un alternant employé par un prestataire informatique d'Adecco, qui a accepté de vendre ses identifiants à un groupe de cybercriminels. Ce geste, en apparence isolé, a permis aux attaquants de pénétrer les systèmes internes et d'exfiltrer un grand volume de données sensibles : informations personnelles, coordonnées bancaires, documents contractuels, etc.

Les conséquences ont été lourdes : **plusieurs victimes** ont été ciblées par des escroqueries sophistiquées, avec des pertes pouvant atteindre **25 000 euros** par personne. Les données volées auraient été revendues sur le dark web ou utilisées dans le cadre de fraudes organisées.

Ce cas illustre de manière frappante l'impact que peut avoir un seul comportement à risque, même au sein d'une grande organisation. Un rappel concret que, dans une organisation, la cybersécurité ne repose pas uniquement sur la technologie mais aussi et surtout sur **les comportements humains**.

 Les points clés à retenir :

- Plus de **70 000 victimes** de vol de données personnelles
- Faille initiale liée à la **vente d'identifiants par un collaborateur**
- Escroqueries jusqu'à **25 000 euros par victime**
- Un exemple concret des **risques humains en cybersécurité**



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.
- Signalez toute anomalie : Si vous remarquez un comportement étrange sur votre ordinateur ou vos outils de travail, avertissez immédiatement votre responsable IT.
- 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.

BlueSecure, Tour Le Belvédère, 1-7 Cr Valmy 92800, PARIS LA DEFENSE, FRANCE

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