

1

Nouveau micro-learning :
Gestionnaire de mots de passe

2

Nouveau micro-learning : SSO

3

Nouveau micro-learning :
Sécuriser ses visioconférences

Bonjour,

Je suis ravie de vous retrouver pour découvrir **les nouveautés du mois d'Octobre !**

Au programme ce mois-ci :

Octobre 2025

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



Nouveau micro-learning - Gestionnaire de mots de passe

Nous enrichissons notre catalogue de formation avec un nouveau module dédié à l'utilisation des **gestionnaires de mots de passe**. Ce contenu pédagogique, court et accessible, explique de manière claire et interactive **ce qu'est un gestionnaire, son utilité et les bonnes pratiques pour l'adopter au quotidien**. Trop souvent négligé, cet outil permet pourtant de créer, stocker et utiliser des mots de passe forts en toute simplicité, tout en réduisant considérablement les risques de compromission. Grâce à des exemples concrets et des conseils pratiques, ce module sensibilise vos collaborateurs à l'importance d'une gestion sécurisée des identifiants et les aide à **renforcer leur sécurité numérique sans complexité**.



Nouveau micro-learning - SSO : se

connecter plus simplement et en toute sécurité

Nouveau module dédié au Single Sign-On (SSO), un mécanisme d'authentification simple et sécurisé, déjà utilisé dans de nombreuses organisations. Ce module pédagogique présente de manière claire et accessible **le fonctionnement du SSO, ses bénéfices en matière de sécurité et les bons réflexes à adopter** pour en tirer pleinement parti. Grâce à ce système, les collaborateurs peuvent accéder à plusieurs applications avec un seul mot de passe, tout en réduisant les risques liés à la gestion des identifiants. Ce micro-learning aide à **comprendre les enjeux de cette authentification centralisée, à adopter les bonnes pratiques** (comme la protection du mot de passe principal ou l'activation du MFA) et à renforcer la sécurité numérique tout en facilitant le quotidien.



🛡️ Nouveau micro-learning - Sécuriser ses visioconférences

Nous poursuivons l'enrichissement de notre catalogue avec un **nouveau module dédié à la sécurité des visioconférences**. Dans un contexte où les réunions en ligne sont devenues la norme, ce micro-learning rappelle de manière claire, concrète et accessible **les risques liés à des pratiques non sécurisées** (liens partagés, absence de mot de passe, partage d'écran mal maîtrisé, etc.) et fournit **les bons réflexes à adopter** avant, pendant et après chaque réunion. Grâce à ce contenu court et illustré d'exemples concrets, vos collaborateurs apprendront à **protéger leurs échanges, leurs données et celles de l'entreprise**, même à distance. Un rappel essentiel à l'heure du télétravail et de la collaboration numérique généralisée.



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 : Bouygues Telecom touché par une cyberattaque massive – 6 millions de comptes clients affectés

Bouygues Telecom, un acteur majeur des télécommunications en France, a récemment été victime d'une **importante cyberattaque** ayant compromis les données personnelles d'environ **6 millions de clients**. Ce cyberincident souligne une nouvelle fois la vulnérabilité des grandes entreprises face aux menaces numériques de plus en plus sophistiquées.

L'attaque a permis aux **cybercriminels d'accéder à des informations sensibles** telles que les noms, prénoms, adresses postales, numéros de téléphone et adresses e-mail des clients. Bien que les données bancaires et les mots de passe n'aient pas été concernés, **cette fuite représente un risque significatif** de phishing ciblé et d'usurpation d'identité.

Ce cas met en lumière l'importance cruciale d'une **vigilance accrue et d'une gestion rigoureuse** des données personnelles dans les infrastructures numériques des opérateurs. Il rappelle aussi la nécessité de disposer d'un plan de réponse rapide pour limiter les impacts sur les

clients et renforcer la confiance.

 Les points clés à retenir :

- Environ **6 millions de comptes clients** affectés
- Données compromises : informations personnelles (nom, adresse, e-mail, téléphone)
- Pas de fuite de données bancaires ou mots de passe déclarée
- 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.
- 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](#)