



1

Formation:
4 nouveaux micro-learnings

2

Campagne de phishing:
Nouveaux scénarios



Nouveaux micro-learnings

Ransomware 15min :

5 chapitres pour comprendre les ransomwares : leur fonctionnement, leurs impacts et les différentes formes d'attaques. La formation vous guide sur les bons réflexes face à une attaque et les signaux d'alerte à repérer pour réagir efficacement.

La cybersécurité en mobilité :

Pourquoi travailler hors du bureau augmente les risques et comment s'en protéger. Mise en avant des bons réflexes sur les appareils, les connexions et la protection des informations dans les lieux publics.

Stress & urgence, l'arme secrète des hackers :

Les cyberattaques jouent sur un levier puissant : l'urgence. En créant stress et pression, elles poussent à agir trop vite et à faire des erreurs. Cette formation vous apprend à reconnaître ces pièges et à reprendre le contrôle avec des réflexes simples de vérification.

Protection des données de santé :

Les données de santé sont parmi les plus sensibles : elles concernent directement l'intimité et la vie privée des personnes et leur mauvaise gestion peut avoir de lourdes conséquences. Cette formation vous apprend à les reconnaître, les manipuler avec précaution et adopter les bons réflexes pour garantir leur confidentialité au quotidien.

[Créer ma campagne learning](#)

Nouveaux scénarios de phishing



Silae - Votre bulletin de paie



Apollo - Merci pour votre fidélité



Armado - Nouvelle connexion



Ameli - Connexion Suspecte



Bouygues - Seuils dépassés



Pluxee - Connexion suspecte

[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 : fuite de données chez Boulangerie Ange — environ 812 000 clients exposés en France

La chaîne de boulangeries **Boulangerie Ange** a été victime d'une **fuite de données importante**, revendiquée autour du 8 mai 2026, touchant environ **812 000 personnes**. L'incident concerne une base de données liée aux services numériques de l'enseigne, incluant des informations utilisées dans le cadre des programmes clients et des commandes en ligne.

Les données exposées comprendraient principalement des informations d'identification et de contact des clients, sans indication confirmée de compromission de données bancaires ou de mots de passe .

L'attaque aurait exploité une faiblesse liée à un accès applicatif (type API ou jeton d'authentification exposé), permettant l'extraction d'une base de données clients. L'incident a été revendiqué sur des forums spécialisés

dans la cybercriminalité, puis relayé par des plateformes de suivi de fuites de données en France

Les points clés à retenir :

- Environ 812 000 personnes concernées
- Fuite de données personnelles de contact (identité + téléphone + ville)
- Incident lié à une base client d'un réseau national de boulangeries

Rappel des bonnes pratiques :

- **Se méfier des appels et SMS frauduleux**
Les données exposées (téléphone, nom, ville) permettent des campagnes de **phishing très crédibles** se faisant passer pour Boulangerie Ange ou un service client.
- **Ne jamais cliquer sur des liens reçus par SMS ou email non vérifié**
Les attaquants peuvent utiliser vos informations personnelles pour vous mettre en confiance.
- **Surveiller les tentatives d'usurpation d'identité**
Même sans données bancaires, ces informations peuvent servir à ouvrir des comptes frauduleux ou réaliser des arnaques ciblées.
- **Utiliser des mots de passe uniques sur les comptes liés**
Si vous avez réutilisé des identifiants ailleurs, changez-les immédiatement.
- **Rester vigilant face à l'ingénierie sociale**
Les cybercriminels exploitent les données fuitées pour rendre leurs messages plus crédibles (ex : "Nous avons votre commande récente...").

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](#)