



Événements

Découvrez les temps forts qui ont marqués ces dernières semaines.



Plateforme

Récapitulatif des publications des derniers trimestres.



Phishing

Les nouveaux scénarios de phishing disponibles.

Mon espace

Récapitulatif des deux premiers trimestres



+30

Nouveautés e-learning et scénarios de phishing



+12

Nouveautés sur la plateforme



+500K

Utilisateurs sensibilisés

Suivez-nous sur LinkedIn

Les temps forts de ces dernières semaines

Juin

Ready for IT

Je sensibilise

CoteR numérique

Résilience Club F24

Plusieurs événements majeurs de l'écosystème cyber. Autant d'occasions d'échanger avec les acteurs du secteur et de découvrir les enjeux de demain



“ Une excellente occasion d'échanger sur les bonnes pratiques et les enjeux de demain. ”

Journée de sensibilisation au Ministère de l'Intérieur



Notre Chatbot disponible sur Teams

Votre assistant cyber disponible dans Teams.

Suivi de son espace apprenant, relances automatiques et signalements.



Personnalisation de la plateforme

Personnalisez la plateforme à votre image avec vos couleurs et votre logo.



Nouvel éditeur IA

Créez vos campagnes en quelques clics avec l'IA.

✓ Génération automatique de contenus (e-mails, SMS, pages, fichiers...)

✓ Optimisation IA (expéditeur, objet, nom, marque...)

✓ Page de destination et post-phishing automatique



Page pédagogique dynamique

Créez des groupes intelligents qui se mettent à jour en temps réel selon vos critères.

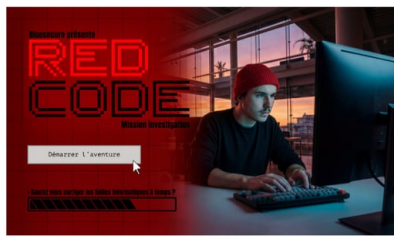


Page pédagogique dynamique

Une page dynamique qui explique le phishing et aide vos utilisateurs à adopter les bons réflexes.

Découvrir les nouveautés





[Découvrir les nouveautés](#)

Nouveaux scénarios de phishing



Netsuite - Avertissement expiration mot de passe



Fedex - Colis reprogrammé



Cloudflare - Accès via IP inconnue



Keeper - Nouvel appareil connecté



DHL - Incident expédition colis



Apple - Renouvellement du matériel

[Créer ma campagne de phishing](#)



JDN 14 NEWS TECH MEDIA START-UP CYBERSÉCURITÉ ACTION PUBLIQUE ÉCONOMIE PLUS

[Cybersécurité](#)

"Vous avez vingt minutes pour reprendre le contrôle" : j'ai testé un jeu vidéo qui simule une crise cyber et voici ce que j'ai vécu

Pascal Collet-Matillon
46 juin 2023 15:30

[Partager](#)



dans la vie réelle.

Une entreprise paralysée et des décisions à prendre dans l'urgence : le serious game BlackOut sensibilise ses joueurs au risque cyber en les confrontant à un ransomware (presque) comme



Suivez notre actualité

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: Une retraitée piégée par un deepfake d'Emmanuel Macron perd 25 000 €



Source : Réseaux sociaux (Reddit / X) – Image générée par IA (deepfake)

Une retraitée de Meurthe-et-Moselle a perdu **25 000 €**, soit l'ensemble de ses économies, après avoir été victime d'une escroquerie utilisant un **deepfake**. Elle avait visionné une fausse publicité mettant en scène **Emmanuel Macron** et **Bernard Arnault**, générée grâce à l'intelligence artificielle, qui faisait la promotion d'une plateforme d'investissement prétendument très rentable.

Convaincue par la vidéo, elle a rempli un formulaire en ligne puis a été contactée par un faux conseiller financier. Après plusieurs versements et de faux gains destinés à gagner sa confiance, elle a investi progressivement toutes ses économies. **Le site frauduleux a ensuite disparu avec son argent.**

- **1 victime** a perdu **25 000 €** dans cette escroquerie.
- **2 personnalités publiques** (Emmanuel Macron et Bernard Arnault) ont été usurpées grâce à un deepfake.
- **1 fausse publicité en ligne** a servi de point d'entrée vers l'arnaque.

🔔 **Rappel des bonnes pratiques :**

- **Méfiez-vous des publicités promettant des gains rapides**
Les offres d'investissement "sans risque" ou aux rendements exceptionnels sont souvent des arnaques.
- **Ne vous fiez pas uniquement à une vidéo**
L'intelligence artificielle permet aujourd'hui de reproduire de manière très réaliste la voix et l'image de personnalités publiques.
- **Vérifiez toujours la plateforme**
Avant d'investir, consultez le site officiel de l'entreprise concernée et recherchez des informations auprès de sources fiables.
- **Ne prenez jamais de décision dans l'urgence**
Les escrocs cherchent souvent à créer un sentiment d'urgence pour empêcher toute vérification.
- **En cas de doute, demandez conseil**
Parlez-en à un proche, à votre banque ou consultez les mises en garde des autorités avant d'effectuer un paiement ou un investissement.

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.