KAIA-OR · NOTE PAR CAS D'UTILISATION

Vérification des fraudes et de l'hameçonnage

Obtenez un second regard sur un message ou un lien avant de répondre, de payer ou de l'ouvrir, et gardez la décision entre vos mains.

IDENTIFIANT DU DOCUMENT	UCB-02-SCAM-AND-PHISHING-CHECKS
VERSION	1.0
DATE	3 novembre 2026
PUBLIC	Particuliers, familles et organisations

En bref

Pour qui	Les particuliers et les familles qui ne savent pas si un message est authentique, et les organisations dont le personnel reçoit des demandes de transfert d'argent ou de modification de la destination des paiements.
Résultat	Un second regard avant que quiconque réponde, paie ou ouvre un lien : les signaux d'alerte que KAIA-OR reconnaît et une prochaine étape suggérée. La décision revient à la personne qui a reçu le message.
Forfait	KAIA-OR Individuel, Famille, Équipe, Entreprise ou Gouvernement

L'enjeu

Pour les particuliers et les familles

Les messages qui se font passer pour un proche, une entreprise de livraison ou une institution financière arrivent par texto, par courriel et par les applications de messagerie, souvent dans plus d'une langue. Leurs signaux d'alerte sont familiers une fois qu'on les connaît : demandes d'identifiants de connexion ou demandes d'argent. La plupart des gens ne se rendent compte qu'un message était faux qu'après avoir répondu ou payé, et l'argent parti est rarement récupéré.

Pour les organisations

Un message annonce que les coordonnées de paiement d'un fournisseur ont changé. Un autre semble provenir d'un membre de la haute direction et demande un transfert d'argent. Les petites équipes n'ont personne en sécurité à consulter, et les grandes ne peuvent pas examiner chaque message que reçoit leur personnel. Le moment de vérifier, c'est avant que quiconque agisse, sans ouvrir le lien.

> En 2025, les personnes qui ont déposé une plainte pour criminalité sur Internet auprès des autorités américaines ont déclaré des pertes de 20,877 milliards de dollars US, en hausse de 26 % par rapport à 2024, et l'hameçonnage et l'usurpation ont été le type de plainte le plus signalé, avec 191 561 plaintes.[1]
>
> Au Royaume-Uni, 43 % des entreprises ont signalé une atteinte à la cybersécurité ou une cyberattaque au cours des 12 mois précédents, et 85 % d'entre elles ont subi de l'hameçonnage.[2]

© Kaia Technologies, Inc.

Ce que KAIA-OR change

Un second regard avant de répondre ou de payer

Collez un message pour voir les signaux d'alerte que KAIA-OR reconnaît. Vous voyez ce qui semble anormal, les cas où la vérification ne peut pas se prononcer et une prochaine étape suggérée, par exemple confirmer par un canal auquel vous faites déjà confiance. La décision vous revient.

Les liens ne sont pas ouverts

Vérifiez un lien sans l'ouvrir. KAIA-OR lit l'adresse et signale ce qui mérite un examen plus attentif avant que quiconque le suive.

Un second regard avant tout paiement

Lorsqu'un message annonce que les coordonnées de paiement d'un fournisseur ont changé, ou semble provenir d'un membre de la direction et demande un transfert d'argent, un membre du personnel le colle et voit les signaux d'alerte et une prochaine étape suggérée avant que quoi que ce soit soit envoyé.

En quatre langues, par écrit ou par la voix

Les vérifications reconnaissent les signaux d'alerte en anglais, en français, en turc et en hébreu. Les personnes qui préfèrent parler peuvent interroger Hey KAIA à voix haute et entendre les signaux d'alerte et une prochaine étape suggérée.

Indicateurs de risque liés aux fichiers et aux logiciels espions

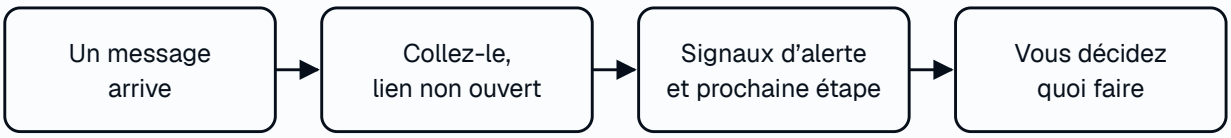
Pour les fichiers et les appareils, KAIA-OR montre des indicateurs de risque qui méritent un examen plus attentif, sans rendre de verdict.

Ce que vous voyez

Élément	Ce qu'il montre
Une vérification de message	Les signaux d'alerte reconnus dans le texte, comme une demande d'identifiants de connexion ou une demande d'argent, les adresses de liens qu'il contient et une prochaine étape suggérée.
Une vérification de lien	Ce qui, dans l'adresse, mérite un examen plus attentif, sans que le lien soit ouvert.
Une vérification de fichier ou de logiciel espion	Des indicateurs de risque qui méritent un examen plus attentif, sans verdict.
Une réponse de Hey KAIA	Ce que le résultat signifie pour vous, à voix haute ou par écrit, avec les données probantes sur lesquelles la réponse s'appuie.

© Kaia Technologies, Inc.

Fonctionnement



La vérification a lieu avant que quiconque réponde, paie ou ouvre un lien.

1. Lorsqu’un message qui semble provenir d’un proche demande de l’argent, vous collez le texte dans la vérification de message avant de répondre.
2. Lorsque le texte contient des demandes d’identifiants de connexion ou des demandes d’argent, le résultat énumère ces signaux d’alerte et les adresses de liens qu’il contient.
3. Lorsqu’un lien vous fait hésiter, vous le vérifiez sans l’ouvrir, et le résultat montre ce qui, dans l’adresse, mérite un examen plus attentif.
4. Si vous préférez parler, vous demandez à voix haute à Hey KAIA ce que signifie le résultat et entendez les signaux d’alerte et une prochaine étape suggérée.
5. Vous joignez le proche par un canal auquel vous faites déjà confiance avant toute autre action. La décision vous revient.

Dans une organisation, la même démarche s’applique lorsqu’un message annonce que les coordonnées de paiement d’un fournisseur ont changé : le membre du personnel le vérifie d’abord, puis joint le fournisseur au moyen des coordonnées que l’organisation possède déjà.

© Kaia Technologies, Inc.

Confidentialité et contrôle

- KAIA-OR vérifie seulement ce que vous choisissez de coller. Il ne lit ni votre boîte de réception ni vos autres applications.
- Les messages et les liens que vous vérifiez restent sur votre appareil.
- Rien n'est transmis à l'IA infonuagique sans votre accord préalable.
- Dans une famille ou une organisation, l'adhésion ne donne jamais accès aux messages, aux appareils, à la position ni aux lieux enregistrés d'un autre membre. Ces limites d'adhésion sont appliquées dans la couche applicative.

Limites, en toute transparence

- Les résultats sont des indicateurs, pas des verdicts. KAIA-OR ne conclut pas à l'absence de danger pour un message, un lien ou un fichier.
- KAIA-OR n'est pas un antivirus, et il ne supprime ni ne modifie quoi que ce soit sur un appareil.
- Il vérifie les messages et les liens que vous choisissez de coller. Il ne prétend pas intercepter les messages de lui-même.
- Les résultats relatifs aux fichiers et aux logiciels espions sont uniquement des indicateurs de risque.

Forfaits et cas d'utilisation connexes

La vérification des fraudes et de l'hameçonnage fait partie des forfaits Individuel, Famille, Équipe, Entreprise et Gouvernement. KAIA-OR fonctionne sur iOS, iPadOS, macOS, les téléphones Android, Android TV, Windows et le Web, en anglais, en français (Canada), en turc et en hébreu. Un même compte fonctionne sur toutes les plateformes, avec les mêmes fonctionnalités et les mêmes règles de confidentialité.

Cas d'utilisation connexes

- Sécurité personnelle
- Sécurité familiale
- Risque numérique et renseignement sur les cybermenaces

© Kaia Technologies, Inc.

Demander un accès anticipé

> L’adhésion se fait sur invitation. Demandez un accès anticipé sur le site Web de KAIA-OR et choisissez le forfait qui vous convient. Les équipes d’entreprise et gouvernementales peuvent aussi utiliser la page Nous joindre du site Web de KAIA-OR.

Sources

1. FBI Internet Crime Complaint Center (IC3), 2025 Internet Crime Report, avril 2026. Contexte du marché uniquement.
2. UK Department for Science, Innovation and Technology (DSIT) with the Home Office, Cyber Security Breaches Survey 2025, avril 2025. Contexte du marché uniquement.

© Kaia Technologies, Inc.

UCB-02-SCAM-AND-PHISHING-CHECKS · Version 1.0 · 3 novembre 2026

La disponibilité des fonctionnalités dépend du forfait et du déploiement. Les fonctionnalités décrites correspondent à la portée engagée du produit KAIA-OR.