KAIA-OR · KULLANIM ALANI ÖZETİ

Dolandırıcılık ve oltalama kontrolleri

Bir mesajı yanıtlamadan, ödeme yapmadan ya da bir bağlantıyı açmadan önce ikinci bir bakıştan yararlanın; karar sizde kalsın.

BELGE KİMLİĞİ	UCB-02-SCAM-AND-PHISHING-CHECKS
SÜRÜM	1.0
TARİH	3 Kasım 2026
HEDEF KİTLE	Bireyler, aileler ve kurumlar

Bir bakışta

Kimler için	Bir mesajın gerçek olup olmadığından emin olamayan bireyler ve aileler ile çalışanları para aktarma ya da paranın gönderildiği yeri değiştirme talepleri alan kurumlar.
Sonuç	Biri yanıt vermeden, ödeme yapmadan ya da bir bağlantıyı açmadan önce ikinci bir bakış: KAIA-OR'un tanıdığı uyarı işaretleri ve önerilen bir sonraki adım. Karar, mesajı alan kişide kalır.
Paket	KAIA-OR Bireysel, Aile, Ekip, Kurum veya Kamu

Zorluk

Bireyler ve aileler için

Bir yakını, bir kargo şirketini ya da bir finans kuruluşunu taklit eden mesajlar kısa mesaj, e-posta ve mesajlaşma uygulamaları üzerinden, çoğu zaman birden fazla dilde gelir. Bu mesajların uyarı işaretleri, bir kez öğrendiğinizde tanıdıktır: giriş bilgisi talepleri veya para istemleri. Çoğu kişi bir mesajın gerçek olmadığını ancak yanıt verdikten ya da ödeme yaptıktan sonra fark eder ve gönderilen para nadiren geri alınabilir.

Kurumlar için

Bir mesaj, bir tedarikçinin ödeme bilgilerinin değiştiğini söyler. Bir başkası üst düzey bir yöneticiden geliyormuş gibi görünür ve para aktarılmasını ister. Küçük ekiplerin danışabileceği güvenlik personeli yoktur; büyük ekipler ise çalışanlarının aldığı her mesajı inceleyemez. Kontrol etmenin doğru anı, bağlantıyı açmadan, kimse harekete geçmeden öncesidir.

> 2025'te ABD makamlarına internet suçu şikâyetinde bulunan kişiler 20,877 milyar ABD doları kayıp bildirdi; bu, 2024'e göre %26'lık bir artıştı. En çok bildirilen şikâyet türü ise 191.561 şikâyetle oltalama ve kimlik sahteciliği (spoofing) oldu.[1]
>
> Birleşik Krallık'taki işletmelerin %43'ü önceki 12 ay içinde bir siber güvenlik ihlali veya saldırısı bildirdi; bu işletmelerin %85'i oltalamayla karşılaştı.[2]

© Kaia Technologies, Inc.

KAIA-OR ile neler değişir

Yanıt vermeden ya da ödeme yapmadan önce ikinci bir bakış

KAIA-OR'un tanıdığı uyarı işaretlerini görmek için bir mesajı yapıştırın. Neyin yolunda görünmediğini, kontrolün emin olamadığı durumları ve zaten güvendiğiniz bir kanaldan teyit etmek gibi önerilen bir sonraki adımı görürsünüz. Karar sizde kalır.

Bağlantılar açılmadan kalır

Bir bağlantıyı açmadan kontrol edin. KAIA-OR adresi okur ve kimse bağlantıya gitmeden önce daha dikkatli bakılması gerekenleri gösterir.

Biri ödeme yapmadan önce ikinci bir bakış

Bir mesaj bir tedarikçinin ödeme bilgilerinin değiştiğini söylediğinde ya da bir yöneticiden geliyormuş gibi görünüp para aktarılmasını istediğinde, çalışan mesajı yapıştırır ve herhangi bir şey gönderilmeden önce uyarı işaretlerini ve önerilen bir sonraki adımı görür.

Dört dilde, yazıyla ya da sesle

Kontroller uyarı işaretlerini İngilizce, Fransızca, Türkçe ve İbranice tanır. Konuşmayı tercih edenler Hey KAIA'ya sesli olarak sorabilir ve uyarı işaretlerini ve önerilen bir sonraki adımı dinleyebilir.

Dosya ve casus yazılım risk göstergeleri

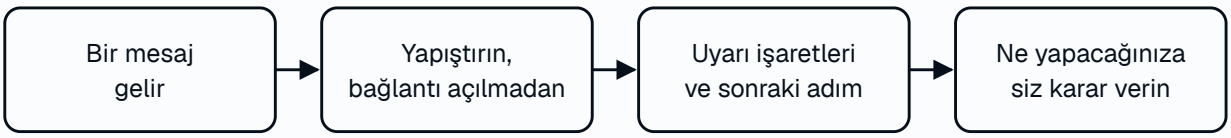
Dosyalar ve cihazlar için KAIA-OR, hüküm vermeden, daha dikkatli bakılmaya değer risk göstergelerini gösterir.

Gördükleriniz

Öğe	Ne gösterir
Mesaj kontrolü	Metinde tanınan, giriş bilgisi talepleri veya para istemleri gibi uyarı işaretleri, metindeki bağlantı adresleri ve önerilen bir sonraki adım.
Bağlantı kontrolü	Adreste daha dikkatli bakılması gerekenler; bağlantı açılmadan kalır.
Dosya veya casus yazılım kontrolü	Hüküm içermeyen, daha dikkatli bakılmaya değer risk göstergeleri.
Hey KAIA yanıtı	Sonucun sizin için ne anlama geldiği; sesli ya da yazılı olarak ve dayandığı kanıtla birlikte.

© Kaia Technologies, Inc.

Nasıl çalışır



Kontrol, biri yanıt vermeden, ödeme yapmadan ya da bir bağlantıyı açmadan önce yapılır.

1. Bir yakınınızdan geliyormuş gibi görünen bir mesaj para istediğinde, yanıt vermeden önce metni mesaj kontrolüne yapıştırırsınız.
2. Metin giriş bilgisi talepleri veya para istemleri içerdiğinde sonuç bu uyarı işaretlerini ve metindeki bağlantı adreslerini listeler.
3. Bir bağlantıdan emin olmadığınızda onu açmadan kontrol edersiniz; sonuç adreste daha dikkatli bakılması gerekenleri gösterir.
4. Konuşmayı tercih ederseniz sonucun ne anlama geldiğini Hey KAIA'ya sesli olarak sorar, uyarı işaretlerini ve önerilen bir sonraki adımı dinlersiniz.
5. Başka bir şey yapmadan önce yakınınıza zaten güvendiğiniz bir kanaldan ulaşırsınız. Karar sizde kalır.

Bir kurumda, bir mesaj bir tedarikçinin ödeme bilgilerinin değiştiğini söylediğinde de aynı akış geçerlidir: çalışan önce mesajı kontrol eder, ardından tedarikçiye kurumun elinde zaten bulunan iletişim bilgileri üzerinden ulaşır.

© Kaia Technologies, Inc.

Gizlilik ve denetim

- KAIA-OR yalnızca yapıştırmayı seçtiğiniz içeriği kontrol eder. Gelen kutunuzu veya diğer uygulamalarınızı okumaz.
- Kontrol ettiğiniz mesajlar ve bağlantılar cihazınızda kalır.
- Siz önce kabul etmedikçe hiçbir şey bulut tabanlı bir yapay zekâ hizmetine gitmez.
- Bir ailede ya da kurumda üyelik, başka bir üyenin mesajlarına, cihazlarına, konumuna veya kayıtlı yerlerine asla erişim hakkı vermez. Bu üyelik sınırları uygulama katmanında sağlanır.

Dürüst sınırlar

- Sonuçlar hüküm değil, göstergedir. KAIA-OR bir mesaj, bağlantı veya dosya için “tehlike yok” sonucu vermez.
- KAIA-OR bir virüsten koruma yazılımı değildir; bir cihazda hiçbir şeyi kaldırmaz veya değiştirmez.
- Yapıştırmayı seçtiğiniz mesajları ve bağlantıları kontrol eder. Mesajları kendiliğinden yakaladığı iddiasında bulunmaz.
- Dosya ve casus yazılım sonuçları yalnızca risk göstergesidir.

Paketler ve ilgili kullanım alanları

Dolandırıcılık ve oltalama kontrolleri Bireysel, Aile, Ekip, Kurum ve Kamu paketlerinin bir parçasıdır. KAIA-OR; iOS, iPadOS, macOS, Android telefonlar, Android TV, Windows ve web’de İngilizce, Fransızca (Kanada), Türkçe ve İbranice çalışır. Tek hesap her platformda aynı özellikler ve aynı gizlilik kurallarıyla çalışır.

İlgili kullanım alanları

- Kişisel güvenlik
- Aile güvenliği
- Dijital risk ve siber tehdit istihbaratı

© Kaia Technologies, Inc.

Erken erişim talep edin

> Üyelik davetle verilir. KAIA-OR web sitesinden erken erişim talep edin ve size uygun paketi seçin. Kurumsal şirketlerdeki ve kamu kurumlarındaki ekipler, KAIA-OR web sitesindeki “Bize ulaşın” seçeneğini de kullanabilir.

Kaynaklar

1. FBI Internet Crime Complaint Center (IC3), 2025 Internet Crime Report, Nisan 2026. Yalnızca pazar bağlamı içindir.
2. UK Department for Science, Innovation and Technology (DSIT) with the Home Office, Cyber Security Breaches Survey 2025, Nisan 2025. Yalnızca pazar bağlamı içindir.

© Kaia Technologies, Inc.

UCB-02-SCAM-AND-PHISHING-CHECKS · Sürüm 1.0 · 3 Kasım 2026

Bir yeteneğin sunulup sunulmadığı pakete ve kuruluma bağlıdır. Yetenekler, KAIA-OR’un taahhüt edilen ürün kapsamı olarak açıklanmıştır.