KAIA-OR · TEKNİK RAPOR · SOSYAL MÜHENDİSLİK

İkinci bir bakış

Ailelerin ve kurumların dolandırıcılığa, kurumsal e-posta dolandırıcılığına ve kimliğe bürünmeye karşı savunması: biri yanıt vermeden, ödeme yapmadan ya da açmadan önce ikinci bir bakış ve insanlarda kalan karar.

BELGE KİMLİĞİ	WP-3
SÜRÜM	1.0
TARİH	3 Kasım 2026
HEDEF KİTLE	Aileler ve bireyler; küçük işletme sahipleri; finans, güvenlik farkındalığı ve risk yöneticileri; kurumsal şirketlerin ve kamu kurumlarının güvenlik ekipleri

İçindekiler

1. Yönetici özeti 3
2. Sorun ve tuzakların işleyişi 4
    1. Sorunun boyutu 4
    2. Günümüzdeki tuzaklar genel hatlarıyla nasıl işler 4
3. İkinci bakış modeli 6
    1. Tek seferlik hükümler neden yetersiz kalır 6
    2. İkinci bakış nasıl işler 6
    3. Bağlam önemlidir 7
4. Aileler ve kurumlar 8
    1. Aileler ve yaşlı yakınlar 8
    2. Kurumlar: fatura sahteciliği, yönetici kimliğine bürünme ve yurt dışındaki personel 8
5. Asistanın kendisini korumak ve dürüst sınırlar 10
6. Kişiler ve kurumlar için bir eylem rehberi 11
7. Bunun sizin için anlamı 12
    1. Terimler sözlüğü 12

© Kaia Technologies, Inc.

Yönetici özeti

Çevrim içi suçlardan kaynaklanan pek çok kayıp teknik bir sızmayla başlamaz. Bir kişinin ikna edilmesiyle başlar: yanıt vermeye, onaylamaya, açmaya, para aktarmaya. Sosyal mühendislik işe yarar; çünkü yazılımı değil muhakemeyi hedef alır ve insanların iş ve aile için kullandığı kanallardan gelir. Yalnız yaşayan yakına, tedarikçi faturalarını işleyen çalışana, seyahatteki yöneticiye ve yurt dışında görevli kamu görevlisine ulaşır.

Pek çok araç ya tek bir öğe hakkında tek seferlik bir hüküm verir ya da kayıp yaşanana kadar hiçbir şey yapmaz. KAIA-OR farklı bir şey sunar: **biri yanıt vermeden, ödeme yapmadan ya da açmadan önce ikinci bir bakış**.

- **Bir mesajı yapıştırın ya da Hey KAIA'ya sesli olarak sorun;** KAIA-OR'un tanıdığı uyarı işaretlerini ve önerilen bir sonraki adımı görün veya dinleyin.
- **Bir bağlantıyı açmadan kontrol edin.**
- **Neyin yolunda görünmediğini ve kontrolün emin olamadığı durumları görün.** Önerilen bir sonraki adım, zaten güvendiğiniz bir kanaldan teyit etmeye yönlendirir. Karar sizde kalır.
- **Kendi dilinizde.** Mesaj kontrolleri uyarı işaretlerini İngilizce, Fransızca, Türkçe ve İbranice tanır.
- **Her kişi için.** Bir ailedeki her yetişkinin ve bir kurumdaki her üyenin kendi cihazında kendi ikinci bakışı vardır. Üyelik, başka bir üyenin mesajlarına asla erişim hakkı vermez.

Bu rapor; sorunun boyutunu, günümüzdeki tuzakların genel hatlarıyla nasıl işlediğini, tek seferlik hükümlerin neden yetersiz kaldığını, ikinci bakış modelinin aileler ve kurumlar için nasıl işlediğini, asistanın kendisinin nasıl korunduğunu, yaklaşımın dürüst sınırlarını ve kişiler ile kurumlar için kısa bir eylem rehberini ortaya koyar.

> **BU RAPOR HAKKINDA**
>
> Bu rapor, KAIA-OR'un tasarımını ve taahhüt edilen ürün kapsamını açıklar. Bir yeteneğin sunulup sunulmadığı pakete ve kuruluma bağlıdır. Gerçek tuzakları öğretmemek veya taklit etmemek için rapor hiçbir zaman dolandırıcılık metinlerine, gerçek markalara veya örnek web adreslerine yer vermez.

© Kaia Technologies, Inc.

1. Sorun ve tuzakların işleyişi

Sorunun boyutu

Birden fazla ülkede kamuya açık raporlar aynı eğilimi anlatır: kayıplar büyüktür, artmaktadır ve merkezlerinde teknik sızma değil, ikna vardır. Aşağıdaki rakamlar pazar bağlamı içindir. Herhangi bir ürünün etkisini değil, bildirilen kayıpları ve olayları anlatır.

DOLANDIRICILIK VE SOSYAL MÜHENDİSLİĞE İLİŞKİN KAMUYA AÇIK RAKAMLAR

Konu	Bildirilen
Bildirilen internet suçu kayıpları, Amerika Birleşik Devletleri	2025'te bildirilen 20,877 milyar ABD doları kayıp; 2024'e göre %26 artış.[1]
En çok bildirilen şikâyet türü, Amerika Birleşik Devletleri	2025'te 191.561 şikâyetle oltalama ve kimlik sahteciliği (spoofing).[1]
60 yaş ve üzerindeki kişilerin bildirdiği kayıplar, Amerika Birleşik Devletleri	2025'te 201.266 şikâyette 7,748 milyar ABD doları kayıp; kayıplar 2024'e göre %59, şikâyetler %37 arttı.[1]
Bildirilen kurumsal e-posta dolandırıcılığı kayıpları, Amerika Birleşik Devletleri	2025'te bildirilen yaklaşık 3,05 milyar ABD doları kayıp.[1]
Bildirilen tüketici dolandırıcılığı kayıpları, Amerika Birleşik Devletleri	Tüketiciler 2025'te 3 milyon dolandırıcılık ihbarında bulundu ve 15,9 milyar ABD doları kayıp bildirdi.[2]
Birleşik Krallık'taki işletmelerin bildirdiği ihlaller ve saldırılar	Birleşik Krallık'taki işletmelerin %43'ü önceki 12 ay içinde bir ihlal veya saldırı bildirdi; bu işletmelerin %85'i oltalamayla karşılaştı.[3]

İki örüntü öne çıkar. Yaşlılar bildirilen kayıpların orantısız bir payını üstlenir ve çoğu zaman onlara yardım edebilecek yakınlarından uzaktadır. Kurumlara ise çoğu zaman önce birini harekete geçmeye ikna eden bir mesaj aracılığıyla ulaşılır.

Günümüzdeki tuzaklar genel hatlarıyla nasıl işler

Tuzakların ifadeleri sürekli değişir. Yapıları ise çok daha az değişir. Aşağıdaki örüntüler, hiçbir gerçek mesaja yer verilmeden genel hatlarıyla anlatılmıştır.

- **Acele.** Mesaj, bir son tarih ya da hemen gerçekleşecekmiş gibi görünen bir sonuçla düşünmeye zaman bırakmaz.
- **Otorite.** Mesaj, üzerinizde yetkisi olan birinden geliyormuş gibi görünür: bir yönetici, bir kamu makamı, bir finans kuruluşu, bir hizmet sağlayıcı.
- **Tanıdıklık.** Tanıdığınız birinden geliyormuş gibi görünür: başı dertte olan bir yakın, bir iş arkadaşı, uzun süredir çalışılan bir tedarikçi.
- **Paranın yeni bir yere aktarılması.** Paranın yeni bir alıcıya gönderilmesi ya da düzenli bir ödemenin gittiği yerin değiştirilmesi talebi.
- **Giriş bilgisi talepleri.** Giriş bilgilerini paylaşma ya da sizin başlatmadığınız bir girişi onaylama talebi.
- **Bir bağlantı ya da dosya.** Gerçek bir sayfayı taklit eden bir sayfa ya da açılmayı bekleyen bir ek.

© Kaia Technologies, Inc.

- **Kanal değişikliği.** Talebin kontrol edilebileceği kanallardan uzaklaşarak yeni bir numaraya, özel bir sohbete ya da bir telefon görüşmesine geçilmesi.
- **Yapay sesler ve yüzler.** Hedef alınan kişinin tanıdığı birini taklit eden, yapay olarak üretilmiş ses veya video.

Tuzakların çoğu bunlardan iki ya da üçünü bir araya getirir. Ortak amaçları, kişiyi muhakeme anından koparmaktır. Bu nedenle işe yarar bir savunma her mesajı tanımaya dayanmaz. İnsanlara, yanıt vermeden, ödeme yapmadan ya da açmadan önce o ana güvenilir biçimde geri dönmenin bir yolunu sunması gerekir.

© Kaia Technologies, Inc.

2. İkinci bakış modeli

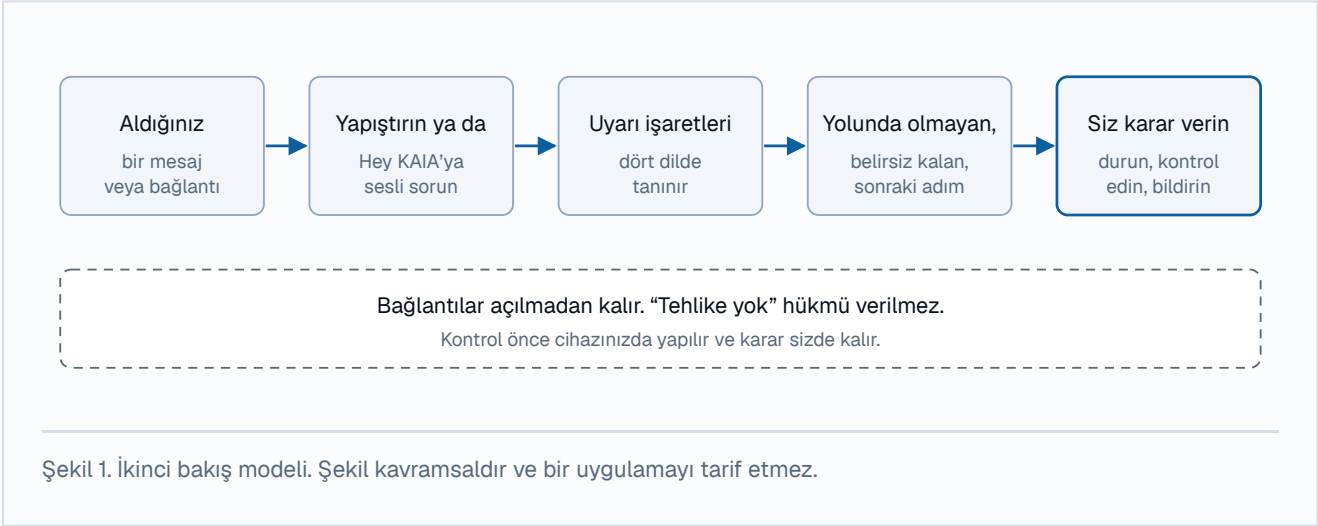
Tek seferlik hükümler neden yetersiz kalır

Şüpheli bir mesaja verilen alışılmış yanıt, tek bir öğe hakkında tek bir hüküm döndüren bir araçtır. Bu yaklaşımın üç zayıf yönü vardır.

- **Yanıltıcı rahatlık.** Hiçbir kontrol aracı tüm tuzakları tanımaz. Yeni bir tuzak hakkında verilen “sorun yok” hükmü izin gibi okunur ve iyi tasarlanmış bir tuzağın elde etmek istediği de tam olarak budur.
- **Bağlam yok.** Yapıştırılan tek bir öğe hakkındaki hüküm, kişinin seyahatlerini, çevresindeki olayları ya da hangi dilde düşündüğünü bilmez.
- **Karar desteği yok.** Bir hüküm “kötü” ya da “sorun yok” der ama bundan sonra ne yapılacağını söylemez; oysa sonucu belirleyen bir sonraki adımdır.

İkinci bakış nasıl işler

KAIA-OR hükmün yerine ikinci bir bakış koyar. Kontrol kişide kalır; ürün, kişinin gözden kaçırmış olabileceklerini görmesine yardımcı olur.



Şekil 1. İkinci bakış modeli. Şekil kavramsaldır ve bir uygulamayı tarif etmez.

- **Yapıştırın ya da söyleyin.** Kişi bir mesajı KAIA-OR’a yapıştırır ya da Hey KAIA’ya sesli olarak sorar; bu da yazmak yerine konuşmayı tercih edenlere kolaylık sağlar.
- **Uyarı işaretlerini görün.** KAIA-OR; giriş bilgisi talepleri veya para istemleri, kanal değişikliği ya da iddia edilen kimlikle uyuşmayan bir gönderici gibi tanıdığı uyarı işaretlerini gösterir.
- **Bağlantılar açılmadan kalır.** Kişi bir bağlantıyı açmadan kontrol edebilir.
- **Neyin yolunda görünmediğini ve kontrolün emin olamadığı durumları görün.** Kanıt yeterli olmadığında KAIA-OR tahmin yürütmek yerine bunu açıkça söyler.
- **Önerilen bir sonraki adım.** Genellikle zaten güvendiğiniz bir kanaldan teyit etmek: elinizdeki bir numara, bildiğiniz bir adres, yüz yüze sorabileceğiniz bir iş arkadaşı. Karar sizde kalır.

Kontroller önce cihazda yapılır. Kişinin kontrol ettiği mesajlar ve bağlantılar kendi cihazında kalır; kişi önce kabul etmedikçe hiçbir şey bulut tabanlı bir yapay zekâ hizmetine gönderilmez.

© Kaia Technologies, Inc.

Bağlam önemlidir

Bir tuzak, ana uyduğunda en ikna edici hâlini alır. Aksayan bir yolculukla ilgili bir mesaj, siz seyahatteyken farklı okunur. Yerel bir acil durumla ilgili bir mesaj, yakınınızda böyle bir durum bildirildiğinde farklı okunur. İkinci bakış, her kişinin kendi seyahat ve olay tablosuyla aynı ürünün içinde yer aldığından kişi, bir mesajın iddia ettiğini olay tablosunun gösterdiğiyle, her olayın ne ölçüde teyit edildiği dâhil, karşılaştırabilir. Bağlam onun yerine karar vermez. Harekete geçmeden önce tartabileceği bir bilgi daha sunar.

© Kaia Technologies, Inc.

3. Aileler ve kurumlar

Aileler ve yaşlı yakınlar

En çok risk altındaki kişi, çoğu zaman zamanında yardım isteme olasılığı en düşük olan kişidir: başka bir şehirde yaşayan yaşlı bir ebeveyn, emin olmadığını söylemekten çekinen bir yakın, İngilizceyi ikinci dil olarak okuyan bir yetişkin. KAIA-OR, satın alan kişinin değil, onların durumu göz önünde bulundurularak tasarlanmıştır.

- **Her yetişkinin kendi kontrolü vardır.** Davet ettiğiniz her yetişkin, ayrı yaşasa bile kendi cihazında kendi KAIA-OR'unu ve kendi ikinci bakışını alır.
- **Kendi dillerinde, sesle.** Bir mesaj bir yakını, bir finans kuruluşunu ya da bir kargo hizmetini taklit ettiğinde her üye mesajı yapıştırabilir ya da Hey KAIA'ya sesli olarak sorabilir ve uyarı işaretlerini ve önerilen bir sonraki adımı İngilizce, Fransızca, Türkçe veya İbranice dinleyebilir.
- **Kimse başkasının mesajlarını okumaz.** Üyelik, başka bir üyenin mesajlarına, cihazlarına, konumuna veya kayıtlı yerlerine asla erişim hakkı vermez. Yardım, başka birinin içeriye bakmasından değil, her kişinin kendi ikinci bakışına sahip olmasından gelir.

Aileler bunu önceden yapılmış basit bir anlaşmayla güçlendirebilir: bir aile üyesinden gelen beklenmedik bir para talebi, o kişiyi talepte verilen bir numaradan değil, her zaman zaten kayıtlı olan bir numaradan geri arayarak teyit edilir.

Kurumlar: fatura sahteciliği, yönetici kimliğine bürünme ve yurt dışındaki personel

Kurumlar için en çok zarar veren tuzaklar, birinin para veya veri aktarma yetkisine sahip olduğu anı hedef alır.

- **Fatura ve tedarikçi sahteciliği.** Tanınan bir tedarikçiden geliyormuş gibi görünen bir mesaj yeni ödeme talimatları bildirir ya da alışılmış faturaya neredeyse benzeyen ama tam olarak aynı olmayan bir fatura gelir.
- **Yönetici kimliğine bürünme.** Üst düzey birinden geliyormuş gibi görünen bir mesaj olağan dışı bir transfer, gizli bir belge ya da alışılmış süreci atlayan bir iyilik ister. Kurumsal e-posta dolandırıcılığının özü budur.
- **Yurt dışındaki personel.** Seyahat eden personel; seyahatini, yerel durumu ya da bir talebi teyit edebilecek iş arkadaşlarından uzakta olmasını istismar eden mesajlar alır.

KAIA-OR, bir kurumun her üyesine, biri ödeme yapmadan önce kendi ikinci bakışını sunar. Değişen bir tedarikçi talimatı ya da olağan dışı bir transfer talebi, uyarı işaretlerini ve önerilen bir sonraki adımı görmek için yapıştırılabilir. Bağlantılar açılmadan kalır. Seyahat eden her çalışan, kendi seyahati için resmî seyahat tavsiyesinde nelerin değiştiğinin yanında, İngilizce, Fransızca, Türkçe veya İbranice kendi ikinci bakışını alır.

Kurum, kişilerin cihazlarının içine bakmadan üyeliğin denetimini elinde tutar. Roller kişileri değil, üyeliği yönetir. Davetler tek kullanımlıktır ve bir hesaba bağlıdır; erişim incelemeleri tarihlidir. Kurum, kişilerin nerede olduğunu değil, kendi tesislerini görür ve üyelerinin kontrol ettiği mesajları okumaz.

© Kaia Technologies, Inc.

SÜREÇ İKNADAN GÜÇLÜDÜR

Fatura sahteciliğine ve yönetici kimliğine bürünmeye karşı en güçlü kurumsal savunma, hiçbir mesajın atlayamayacağı bir süreçtir: paranın gideceği yerde yapılacak bir değişiklik, kayıtlarda zaten bulunan bir irtibat kişisi üzerinden teyit edilir; büyük veya olağan dışı transferler için de ikinci bir kişinin onayı gerekir. İkinci bakış bu süreci destekler; onun yerini almaz.

© Kaia Technologies, Inc.

4. Asistanın kendisini korumak ve dürüst sınırlar

Yapay zekâyı hedef alan sosyal mühendislik. Asistanlar insanların aldığı içeriğin daha fazlasını okudukça saldırganlar kişi yerine asistanı ikna etmeye çalışır. Bir mesaj, bir sayfa ya da bir belge, bir asistana kurallarını yok saydırmak, bilgi açıklatmak ya da bir işlem yaptırmak amacıyla gizlenmiş talimatlar içerebilir. Hey KAIA buna direnecek şekilde tasarlanmıştır. Kontrol etmesi istenen içerik, izlenecek talimatlar olarak değil, her zaman incelenecek veri olarak ele alınır. Model çıktısı hiçbir yetki vermez: bir yapay zekâ modelinin ürettiği hiçbir şey bir işlemi onaylayamaz, bir izni değiştiremez ya da bir otomatik aracın yapabileceklerini genişletemez. Yanıtlar siz görmeden önce kanıtla karşılaştırılır ve bu kanıtı belirtir. Hiçbir tasarım manipülasyon olasılığını tamamen ortadan kaldıramaz; bu nedenle son güvence, KAIA-OR'un diğer her yerinde olduğu gibidir: karar insanlarda kalır.

Dürüst sınırlar. İkinci bakış, ne olduğu konusunda dürüst olduğu için işe yarar.

- **Hüküm değil, gösterge.** KAIA-OR uyarı işaretlerini gösterir ve bir sonraki adımı önerir. Bir mesajın zararsız olduğunu asla ilan etmez; uyarı işareti bulunmaması da "tehlike yok" anlamına gelmez.
- **Ona verdiğinizi kontrol eder.** Mesajları veya bağlantıları siz görmeden önce yakalamaz ve tüm dolandırıcılıkları tanıdığını iddia etmez.
- **Virüsten koruma yazılımı değildir.** Dosya ve casus yazılım kontrolleri yalnızca risk göstergeleri sunar, hiçbir zaman hüküm vermez.
- **Emin olamadığında bunu söyler.** Bazı mesajlar yalnızca içeriklerine bakılarak değerlendirilemez. KAIA-OR bu durumda bunu söyler ve önerilen bir sonraki adım, zaten güvendiğiniz bir kanaldan teyit etmektir.
- **Bir kaybı geri alamaz.** İkinci bakış, kişi yanıt vermeden, ödeme yapmadan ya da açmadan önce gelir. KAIA-OR gönderilmiş parayı geri getiremez.

© Kaia Technologies, Inc.

5. Kişiler ve kurumlar için bir eylem rehberi

Çoğu durumu üç adım karşılar: durun, zaten güvendiğiniz bir kanaldan kontrol edin ve bildirin. Bunlar yalnızca siber güvenliğe yönelik sonraki adımlardır. Doğal tehlikeler ve kamu güvenliği olayları için yayımlayan kurumun yönlendirmesini izleyin.

DURUN, KONTROL EDİN, BİLDİRİN

Adım	Bir kişi veya aile için	Bir kurum için
Durun	Düşünmeye zaman bırakmayan bir talebi başlı başına bir uyarı işareti olarak görün. Emin değilken yanıt vermeyin, ödeme yapmayın ve açmayın.	Kimden geliyormuş gibi görünürse görünsün, olağan dışı bir talep üzerine harekete geçmeden önce durup sormayı çalışanlar için olağan ve memnuniyetle karşılanan bir davranış hâline getirin.
Kontrol edin	İkinci bir bakış için mesajı KAIA-OR'a yapıştırın ya da Hey KAIA'ya sesli olarak sorun. Bir bağlantıyı açmadan kontrol edin. Göndericiye, mesajda verilen bir numara veya adresle değil, her zaman elinizde zaten bulunan bir numara veya adres üzerinden ulaşın.	Paranın gideceği yerde yapılacak her değişikliği kayıtlarda zaten bulunan bir irtibat kişisi üzerinden teyit edin. Büyük veya olağan dışı transferler için ikinci bir kişinin onayını şart koşun. Yurt dışındaki personel dâhil her üyeye kendi ikinci bakışını sunun.
Bildirin	Kimliğine bürünülen kuruluşa resmî kanalları üzerinden haber verin ve dolandırıcılığı ülkenizdeki yetkili makamlara bildirin.	Güvenlik irtibat kişinize bildirin, uyarı işaretlerini iş arkadaşlarınızla paylaşın ve erişimi tarihli erişim incelemeleriyle düzenli olarak gözden geçirin.

İyi bir eylem rehberi, stres altında hatırlanabilecek kadar kısadır. Amaç herkesi tuzaklar konusunda uzman yapmak değildir. Amaç durmayı, güvenilir bir kanaldan kontrol etmeyi ve bildirmeyi, ikinci bir bakış el altındayken alışkanlık hâline getirmektir.

© Kaia Technologies, Inc.

Bunun sizin için anlamı

Bireyler ve aileler. Yanıt vermeden, ödeme yapmadan ya da açmadan önce mesajı yapıştırın ya da Hey KAIA'ya sesli olarak sorun; uyarı işaretlerini ve önerilen bir sonraki adımı kendi dilinizde görün. Ailenizdeki her yetişkin kendi KAIA-OR'unu korur.

Ekipler ve küçük işletmeler. Biri ödeme yapmadan önce ikinci bir bakış: değişen bir tedarikçi talimatı ya da olağan dışı bir transfer talebi, bağlantılar açılmadan, önce kontrol edilebilir.

Kurumsal şirketlerin ve kamu kurumlarının güvenlik ekipleri. Yurt dışındaki personel dâhil her çalışanın dört dilde kendi ikinci bakışı vardır. Model çıktısı hiçbir yetki vermez; kurum, kişilerin nerede olduğunu değil, kendi tesislerini görür. KAIA-OR'u değerlendirmek için KAIA-OR web sitesinden erken erişim talep edin ya da "Bize ulaşın" seçeneğini kullanın.

Terimler sözlüğü

Terim	Bu rapordaki anlamı
Sosyal mühendislik	Bir kişiyi, örneğin yanıt vererek, onaylayarak, açarak ya da para aktararak kendi çıkarına aykırı davranmaya ikna etmek.
Kurumsal e-posta dolandırıcılığı	Bir mesajın, parayı başka yere yönlendirmek ya da veri elde etmek için bir yöneticinin, iş arkadaşının veya tedarikçinin kimliğine büründüğü dolandırıcılık.
İkinci bakış	KAIA-OR'un bir mesaj veya bağlantı için yaptığı kontrol: tanıdığı uyarı işaretleri, emin olamadığı noktalar ve önerilen bir sonraki adım.
Uyarı işareti	Giriş bilgisi talepleri veya para istemleri gibi, tuzakların çoğunda ortak olan bir mesaj özelliği.
Gizlenmiş talimatlar	Bir yapay zekâ asistanını manipüle etmek için içeriğe yerleştirilmiş metin. KAIA-OR bu tür içeriği talimat olarak değil, her zaman veri olarak ele alır.

Kaynaklar

1. FBI Internet Crime Complaint Center (IC3), 2025 Internet Crime Report, Nisan 2026. Yalnızca pazar bağlamı içindir.
2. Federal Trade Commission (FTC), FTC Testifies before the Joint Economic Committee on Agency's Efforts to Combat Fraud, Mart 2026. Yalnızca pazar bağlamı içindir.
3. 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.

WP-3 · Sürüm 1.0 · 3 Kasım 2026

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