FRAUD SÖZLÜĞÜ

Dolandırıcılığın dilini öğrenin"

by formica.ai

Anomali Tespiti

Veri madenciliğinde anormallik tespiti, beklenen bir modelden veya verilerin çoğundan ayrılan veri noktalarının, öğelerin, gözlemlerin veya vakaların tanımlanmasıdır.

Bu anormallikler, dolandırıcılık, siber saldırı veya metinlerdeki hatalar gibi bir uyarı sinyali verebilir.

Akış Verileri

Gerçek zamanlı olarak elde edilen verilerin alınması, gönderilmesi ve işlenmesi sürecidir. Yapay zeka desteğiyle bilgiyi işleme ve analiz etme yeteneği, sürecin sürdürülebilir olmasını sağlar.

Çevrimiçi oyunlar, borsalar, işleme tesisleri, perakende yönetim sistemleri ve konum paylaşım uygulamaları, veri akışı uygulamalarına örnektir.

Banka Kimlik Numarası

Kredi kartlarının ilk 6 hanesi banka kimlik numarasıdır (BIN). Bu numara seti, kartı veren finans kuruluşunu tanımlar.

BIN'ler, kart sahiplerinin bulunduğu coğrafi bölgeyi doğrulamak için kullanılır.

Biyometrik Kimlik Doğrulama

İnsanların biyolojik özelliklerine dayalı bir doğrulama veya güvenlik sürecidir.

Örnek olarak yüz tarama, parmak izi doğrulama, göz tarama verilebilir.

Bot Saldırıları

Bot saldırısı, bir web sitesini, uygulamayı, API'yi veya son kullanıcıyı kandırmak, dolandırmak veya utandırmak için kullanılan otomatik web istekleridir.

Basit spam saldırıları olarak başlamış ve daha sonra ekonomileri ve altyapıları ile gün geçtikçe karmaşık yapılara dönüşmüşlerdir.

CNP Dolandırıcılığı

Kartın mevcut olmadığı bir işlem, müşterinin satın alma işlemi sırasında kredi kartını fiziksel olarak göstermediği, posta, telefon veya çevrimiçi olarak bir satın alma işlemi yaptığında gerçekleşir. Bu ödeme yöntemi müşteriler için kolaydır ancak dolandırıcılığa karşı savunmasızdır.

CVV

CVV'ler, kart sahipleri ve satıcılar için ekstra bir güvenlik katmanı sağlayan üç veya dört basamaklı sayılardır.

E-ticarette perakendeciler, satın aldıkları karta sahip olup olmadıklarını doğrulamak için müşterilerden CVV değerini isterler.

Çağrı Merkezi Dolandırıcılığı

Çağrı merkezi dolandırıcılığı, dolandırıcıların gerçek bir müşterinin hesabını ele geçirmek veya kişisel bilgilerini elde etmek için çağrı merkezlerini arayıp gerçek müşterilerin kimliğine bürünmesidir.

Denetimsiz Makine Öğrenimi

Genellikle büyük miktarda etiketlenmemiş verideki kalıpları keşfetmek için kullanılır. Özellikle yeni ve bilinmeyen kalıpları keşfetmede etkilidir.

Anomali tespit tekniklerinde girdi verileri arasındaki ilişkileri incelemeye odaklanır.

Derin Öğrenme

Makine öğreniminin bir alt kategorisi olan Derin Öğrenme, makinelerin karmaşık görevleri programlamaya gerek kalmadan çözmeyi öğrenmesini sağlayan bir yapay zeka türüdür.

Ne kadar çok veri girişi olursa, derin öğrenme süreçleri o kadar başarılı olur.

Doğrulama

Bir işlemin olması gerektiği şekilde ve yapması gereken kişi tarafından yapıldığının doğrulanmasıdır.

Dolandırıcılık önlemede güvenlik amaçlı birçok doğrulama yöntemi vardır.

Dolandırıcılık

Dolandırıcılık, başkalarını aldatarak failin kazancına veya mağdurun zararına neden olan kasıtlı eylemler veya başarısızlıklardır.

Etik olmayan yollarla yürütülür. Bir kişi veya kurumu hak ettiği menfaatlerden mahrum etmek de dolandırıcılık olarak tanımlanmaktadır.

Dolandırıcılık Grafiği

Geleneksel ilişkisel veritabanları, farklı varlıklar arasındaki bilgileri depolama ve analiz etme verimliliğinden yoksundur. Veri içindeki ilişkileri keşfetmek ve görselleştirmek ve ilişkisel veritabanlarının düşük performansının üstesinden gelmek için grafik veritabanlarını kullanmanız gerekir. Kullanıcılar arasındaki ortak telefon numaralarını, e-posta adreslerini belirleyebilir, dolandırıcılığı tespit etmek için analiz edilebilecek benzer bilgilerden oluşan bir ağ oluşturabilirsiniz.

Fidye Yazılımı

Kullanıcıya şantaj yapan kötü amaçlı yazılımardır. Belirli şifrelemeler yaparak bir ücret ödenmedikçe bir bilgisayara erişimi engeller.

Dolandırıcılar genellikle kurbanları önemli verileri silebileceklerini söyleyerek tehdit eder.

Gerçek Zamanlı Dolandırıcılık Analizi

Tüm işlemleri gerçek zamanlı analiz eder ve dolandırıcılık analistlerini olası dolandırıcılık faaliyetlerine karşı uyarır. Geleneksel dolandırıcılık tespit sistemlerinin, anormal etkinliği belirlemek için verileri dönüştürmesi ve analiz etmesi saatler alabilir. Yapay zeka destekli dolandırıcılık tespit hizmetleri, gerçek zamanlı dolandırıcılık tespiti için verimli sonuçlar sağlar

Haksız Rekabet

Piyasa rekabetini teşvik eden yasaların ihlali, kuruluşlar tarafından yürütülen rekabete aykırı ve haksız uygulamaların düzenlenmesidir.

Örneğin; fiyatları sabitleme, ayrımcı fiyatlandırma, haksız ticaret koşulları sağlama.

Hayali Geri Ödemeler

Hayali bir geri ödeme planında, bir çalışan, gerçek bir iade olmamasına rağmen müşteri malı iade ediyormuş gibi davranır.

İşlem gerçek olmadığı için fiili iade yoktur ve böylece şirket envanteri kabartılır.

Hizmet Reddi Saldırısı (DDoS)

Gerçek kullanıcıların bilgisayar korsanları tarafından hizmet almasının engellendiği bir saldırı kategorisidir. Bu saldırılarda, bilgisayar korsanı ağdan veya sunucudan kabul edilemez varış adresleri ile gereksinimleri doğrulamasını isteyen birden fazla mesaj gönderir.
Bu, sistemi aşırı yükleme yapar ve gerçek kullanıcıların bu hizmete erişmesini engelleyebilir.

Hız

Belirli bir kaynaktan gerçekleştirilen işlem hacminin, ortalama kullanıcı hacminden çok fazla olması anlamına gelir. Örneğin uzun süredir kullanılmayan bir hesaptan çok sayıda işlemin aynı anda yapılması Velocity'ye örnektir. Bir kullanıcının birden fazla işleminin hızını ölçmek olarak da tanımlanabilir.

İkili Sınıflandırma

Bir gruba ait elemanların bir sınıflandırma kuralı ile iki gruba ayrılmasıdır. Tipik olarak normal durumu temsil eden bir sınıf ve anormal durumu temsil eden bir sınıf içerir. Kredi kartı hileli işlem tespit yöntemlerinde sıklıkla kullanılmaktadır.

İşlem Kimlik Doğrulama Numarası

Çevrimiçi işlemleri işlemek için kullanılan tek kullanımlık bir koddur. Bir hesaba giriş yapmak veya bir hesapta işlem yapmak için parolaya ek bir güvenlik katmanı sunar.

İşlemlerde dolandırıcılık olasılığını azaltmak için kullanılır.

İşlem İzleme

Bir bilgi sistemi veya iş uygulaması üzerinde yürütülen bir işlemin mevzuat veya politikalara uygunluğunu değerlendirmek için analiz etme ve gözden geçirme süreci.

İzleme

Bir işlemin, müşterinin veya başka herhangi bir şeyin belirli bir süre içindeki ilerlemesini gözlemleme sürecidir.

Sahtekarlık tespit sürecinde genellikle şüpheli işlemler ve müşteriler için yapılır.

İki Faktörlü Kimlik Doğrulama

Çevrimiçi hesapların güvenliğini sağlamak için kullanılan bir araçtır. Kullanıcıya ve şifreye bir güvenlik katmanı eklenerek oluşturulur.

Ancak gelişmiş dolandırıcılık teknolojileri ile iki faktörlü kimlik doğrulamanın bile üstesinden gelinebilir.

Kamu Hizmeti Dolandırıcılığı

Herhangi bir hizmetten yararlanmak için başka birinin adının veya kimliğinin hileli kullanımı.

En yaygın biçim, dolandırıcılık amacıyla kamu görevlilerinin kimliğine bürünmek için telefon görüşmeleri yapmaktır.

Kara Para Aklama

Dolandırıcılık veya herhangi bir yasa dışı yolla elde edilen paranın kaynağının gizlenmesi işlemidir.

Genellikle büyük miktarda para vardır ve tespit, tipik bir dolandırıcılık vakasından daha uzun izleme ve analiz süreçleri gerektirir.

Kural Tabanlı Dolandırıcılık Tespiti

Kural tabanlı dolandırıcılık tespit sistemleri, önceki dolandırıcılık vakalarından elde edilen içgörülerle olası dolandırıcılık eylemlerini belirlemek için verilerin korelasyonunu, istatistiklerini ve mantıksal karşılaştırmasını kullanır.
Genellikle geleneksel veri analizi yöntemlerini kullanırlar ve zaman alıcı araştırma gerektirirler.

Kimlik Avı Saldırıları

Bir dolandırıcının meşru bir kişinin kimliğine bürünerek bir kurbandan özel bilgiler elde etmeye çalışması sürecidir.

E-posta, dolandırıcıların kimlik avı saldırılarında kullandığı en yaygın araçlardan biridir.

Makine Öğrenmesi

Deneyim yoluyla otomatik olarak öğrenmek için verileri analiz eden bir tür yapay zeka.

Makine öğrenimi algoritmaları, programlamaya gerek kalmadan tahminler ve kararlar almak için örnek verileri kullanarak bir model oluşturabilir.

Manuel İnceleme

Herhangi bir yazılım yardımı olmadan risk ekipleri tarafından dolandırıcılık tespitinde yapılan işlemlerin manuel olarak incelenmesi işlemidir.

Bazı durumlarda dolandırıcılık tespit araçları ile yapılan incelemelere ek olarak yapılabilmektedir.

Muhasebe Dolandırıcılığı

Finansal verilerin, kuruluşun gerçek değerini veya finansal faaliyetlerini yansıtmayacak şekilde değiştirilerek sunulduğu durumdur.

Bu, muhasebe suistimalini, hileli borçlanmaları, finansman sağlamayı, hileli uygulamaları ve yasa dışı işlemleri içerebilir.

Müşteri Dolandırıcılığı

Müşteriler veya başkaları tarafından ürün veya hizmetlere yasa dışı erişim ve hileli uygulamalar yoluyla şirketlere yönelik dolandırıcılık uygulamaları.

Ölçeklenebilir Yapay Zeka

Algoritmaların, verilerin, modellerin ve altyapının verilen görev için gereken boyut, hız ve karmaşıklıkta çalışabilme yeteneği olarak tanımlanır.

P2PE

P2PE, kredi kartı işlemlerinin güvenliğini artırmak için oluşturulmuş bir standarttır. Bu standartlara göre iş yeri satış noktasına girilirken işlem verileri güvenli bir şekilde şifrelenir ve bu şifreleme kredi kartı ile yapılan işlemlerin sonuna kadar devam eder. Bu koruma katmanı, SSL şifrelemesine ek olarak kullanılır.

Paket Çözümleyicisi

Verilen ağ üzerinden geçen tüm veri paketlerinin izlenmesi ve yakalanması işlemidir. Yetkisiz bir tarafça bunu yapmak yasa dışıdır. Çalınan bilgiler, dolandırıcılık ve şantaj için kullanılma riskini taşır.

Ağ yöneticileri tarafından ağ trafiğini izlemek ve sorunları gidermek için kullanılırlar.

Risk Değerlendirmesi

Öngörülen bir faaliyet için oluşabilecek potansiyel risklerin değerlendirilmesi sürecidir. Risk değerlendirmesi yapmak için farklı sistem ve yöntemler gerekebilir.

Bu değerlendirme süreci, gelecekte sistemleri tehdit edebilecek risklerin olasılıklarının belirlenmesini de içerir.

Sentetik Kimlik Hırsızlığı

Ağırlıklı olarak başvuru dolandırıcılığı için kullanılan bir teknik olarak bilinmektedir.

Kötü niyetli bir kişinin, birden fazla kişiye ait kişisel verileri içeren bir kimlik oluşturması veya gerçek ve sahte kişisel verilerin bir kombinasyonunu kullanarak bir kimlik oluşturma işlemidir.

Siber Suç

Bir bilgisayar ve bilgisayar ağı tarafından işlenen herhangi bir suçu ifade etmek için kullanılır.

Bilgisayar bir suç aracı olarak kullanılabilir veya bir suçun kurbanı olabilir. Siber suç, bireylerin verilerine ve finansal güvenliğine zarar verebilir.

Sesli Kimlik Avı

Dolandırıcıların sentetik sesler oluşturarak veya birilerini taklit ederek ulaşabilecekleri alanlara erişimidir.

Genellikle başkasının sesini kullanma yöntemi ile karşı tarafı sindirmek amaçlanır.

Sesli Yetkilendirme

Belirli bir işlemin kimliği doğrulanmış bir kişi tarafından gerçekleştirilebilmesini sağlamak için kullanılan bir güvenlik korumasıdır.

Genellikle satın alma aşamalarında yetkili kişinin tanımlanan sesle işleme devam etmesi sağlanarak yapılır.

Tahmine Dayalı Analitik

Tahmine dayalı analitik, mevcut verilere dayalı olarak kullanıcı davranışlarını tahmin eder.

Veriler ile olası olasılıkları değerlendirir ve kullanıcıların olası davranışlarını tahmin ve analiz eder.

Tedarik Dolandırıcılığı

Tedarikçilerin hizmet, mal veya varlıklarının satın alma süreçlerinde teklif verme veya ihale süreçlerini olumsuz etkileyen yasa dışı eylemlerdir.

URL Kısaltıcı Spam

URL kısaltma hizmetleri aracılığıyla kötü amaçlı bağlantıların maskelenmesidir.

Bu tekniğin amacı, spam bağlantılarının güvenli görünmesini sağlamak ve kurbanları bağlantılara tıklamaları için kandırmaktır.

Veri Artırma

Veri artırma, veri analizinde orijinal verileri değiştirerek veri miktarını artırmak için yeni veri noktaları oluşturma işlemidir.

Mevcut eğitim verilerinde bazı değişiklikler yaparak yapay kopyalar oluşturur. Bu kopyalar, mevcut eğitim veri setine eklenerek daha büyük eğitim veri seti oluşturur.

Veri İhlali

Veri ihlali, hassas, gizli veya korunan verilere yasa dışı olarak erişilmesi veya açıklanmasıdır.

Bilgisayar korsanları, zayıf parolalar, kimlik avı saldırıları, yazılım hataları gibi birçok neden veri ihlaline neden olabilir.

Veri Madenciliği

Sonuçları tahmin etmek için büyük veri kümeleri içindeki anormallikleri ve kalıpları bulma sürecidir.

Veri madenciliği, ilgili verileri anlamanıza ve sonuçları değerlendirmenize olanak tanıyarak bilinçli kararlar vermenizi sağlar.

Veri Analizleri

Bir dizi veriyi analiz etmek için makine öğrenimi ve yapay zeka teknolojisini kullanarak elde edebileceğiniz belirli bir iş olgusunun anlaşılmasını ifade eder.

Vergi Kaçakçılığı

Bir kuruluşun veya bireyin vergi borcunu ödememek için kasten kullandığı yasa dışı yöntemlerdir.

Yapay Zeka (YZ)

Yapay zeka, bir bilgisayar programının veya makinesinin düşünme becerilerine ve öğrenme yeteneğine sahip olduğu teknolojidir.

Verileri analiz ederek öğrenen ve veriler aracılığıyla öğrendiklerine göre kendini uyarlayan bir teknolojidir.

Yanlış-Pozitif

Şüpheli olarak tanımlanan ancak henüz doğrulanmamış işlemler dolandırıcılık tespitinde yanlış pozitif olarak değerlendirilir.

Yanlış pozitifler, hem kısa hem de uzun vadede şirketlere büyük mali ve itibar kayıplarına neden olabilir.

Yetkisiz Para Çekme

Bir kişinin yetkisi veya onayı olmaksızın bir kişinin banka hesabından para çekilmesi veya herhangi bir transfer işlemidir.