



EYLÜL 2026 · FARKINDALIK SERİSİ

OKULA DÖNÜŞTE DİJİTAL GÜVENLİK

2026'nın Yeni Tehditleri

Deepfake artık ses taklidiyle de yapılıyor · Yapay zeka sohbet botları ve sahte samimiyet
Sosyal medyada zorbalık ve yaş sınırı tartışmaları · Mesajlaşma ve grup sohbetlerindeki riskler
Yapay zeka ile hazırlanan ödevlerde bilgi kirliliği · Ekran süresiyle sağlıklı denge kurmanın yolları

SPARTA SİBER GÜVENLİK

Bu Sayıda

Sparta Siber Güvenlik, kuruluşların siber güvenlik ihtiyaçları için 2013 yılında kurulmuştur. Bugüne kadar 1000'in üzerinde siber güvenlik danışmanlığı, eğitimi ve sızma testi projesi gerçekleştirmiştir. Bu farkındalık serisiyle, hem bireylerin hem de kurumların gündelik hayatta karşılaştığı güncel siber tehditleri aylık olarak ele alıyoruz.

Bu ay okula dönüş dönemiyle birlikte çocukların ve gençlerin dijital hayatında öne çıkan yeni tehditleri inceliyoruz. Gerçek zamanlı ses taklidiyle üretilen deepfake içerikleri, yapay zeka sohbet botlarının kurduğu sahte samimiyeti, sosyal medyada zorbalığı, mesajlaşma uygulamalarındaki riskleri, yapay zekayla hazırlanan ödevlerde bilgi güvenilirliğini ve ekran süresi sağlıklı bir denge kurmanın yollarını bir araya getirdik.

Okula dönüşte ekranların gölgesi	3
Deepfake artık sadece görüntü değil	4
Deepfake mi? Nasıl anlaşılır?	5
Yapay zeka sohbet botları ve sahte samimiyet	6
Gerçek vaka: Bir sohbet botuyla derinleşen duygusal bağ	7
Sosyal medyada zorbalık	8
Bir çocuk zorbalık yaşadığını anlatırsa	9
Özel mesajlar ve grup sohbetlerindeki riskler	10
Kırmızı bayraklar	10-11
Yapay zeka ile hazırlanan ödevler ve bilgi kirliliği	12
Yapay zekadan alınan bilgi nasıl kontrol edilir?	12-13
İnternette görülen videoların doğruluğu	14
Beş adımda doğrulama	15
Ekran süresi ve kullanım biçimi	16
Aynı süre, farklı etki	17
Fark etme rehberi	18
Güvenli dijital kullanım için üç temel adım	19
İzlenecek müdahale akışı	20
İletişim, kaynakça ve yasal uyarı	21

GİRİŞ

Okula Dönüşte Ekranların Gölgesi

Bu yıl okula dönüş, çanta, defterler ve kalemlerden ibaret değil. Çocukların ve gençlerin gündelik hayatına artık yapay zeka destekli sohbet uygulamaları, sesi taklit edebilen araçlar ve yaş doğrulamasının hala tartışıldığı platformlar da dahil oluyor.

Ekranların çocukların hayatındaki payı yalnızca artmıyor, biçim olarak da değişiyor.



Bir çocuğun bugün karşılaştığı bir sohbet ekranı, birkaç yıl öncekinden çok farklı bir şey ifade ediyor. Karşı taraftaki ses tanıdık bir arkadaşına benzeyebilir, ama aslında yapay zeka tarafından üretilmiş olabilir. Bir mesajlaşma uygulamasında güvenilir görünen bir kullanıcı, hiç tanımadığı biri olabilir. Bir ödev için baktığı kaynak, hiç var olmamış bir kitaba ait çıkabilir. İzlediği bir video, hiç yaşanmamış bir olayı anlatıyor olabilir.

Bu farkındalık serisinin bu sayısında, okula dönüş döneminde çocukların ve gençlerin karşılaştığı bu yeni katmanı ele alıyoruz. Sesi taklit eden yapay zeka araçlarından çocuklarla sahte bir yakınlık kuran sohbet botlarına, sosyal medyada süregelen zorbalıktan mesajlaşma uygulamalarındaki risklere, ödevlerde yapay zekanın ürettiği yanlış bilgilerden gerçeğiyle sahtesi kolay ayırt edilemeyen videolara kadar geniş bir alanı kapsıyoruz. Son bölümde ise bütün bunların ortasında ailelerin ve öğretmenlerin neye dikkat etmesi gerektiğini bir araya getiriyoruz.

Amacımız korku yaratmak değil. Ailelerin ve eğitimcilerin bu yeni araçları tanıyarak çocukları daha bilinçli bir şekilde koruyabilmesini sağlamak istiyoruz.

DEEPFAKE

Deepfake Artık Sadece Görüntü Değil



Deepfake denince çoğumuzun aklına sahte videolar geliyor. Oysa 2026 itibarıyla yapay zeka yalnızca görüntü üretmiyor. Birkaç saniyelik ses kaydından bir kişinin sesini öğrenebiliyor, o kişi gibi konuşabiliyor ve bunu gerçek zamanlı olarak yapabiliyor.

Bu nedenle artık yalnızca gördüklerimize değil, duyduklarımıza da temkinli yaklaşmak gerekiyor. Bu gelişme özellikle çocukların yoğun kullandığı oyun ve sohbet platformlarında yeni riskler ortaya çıkarıyor.

World Economic Forum'da yayımlanan bir değerlendirmeye göre, yetişkinler yapay zeka destekli ses teknolojileriyle çocuk sesi kullanarak oyun içi sohbetlerde ve sosyal platformlarda çocuklarla iletişim kurabiliyor.

WORLD ECONOMIC FORUM, NİSAN 2026

Çocuklar dijital ortamda yeni arkadaş edinmeye daha açık oldukları ve karşılarındaki kişinin gerçekten kim olduğunu doğrulama imkanları sınırlı olduğu için bu tür yöntemlere karşı daha savunmasız olabiliyor. Bu nedenle tanımadıkları kişilerle sesli görüşme yapmamaları, kişisel bilgilerini paylaşmamaları ve rahatsız oldukları her durumu aileleri veya öğretmenleriyle paylaşmaları büyük önem taşıyor.

Artan riskler nedeniyle platformlar da yeni önlemler almaya başladı. Ancak teknoloji ne kadar gelişirse gelişsin, çocukların dijital güvenliğinde en etkili koruma hala bilinçli kullanım ve aile rehberliği olmaya devam ediyor.

DEEPFAKE

Şüpheli bir ses veya görüntüyle karşılaştığınızda izlenebilecek dört basit adım:

ŞÜPHELİ SES VEYA GÖRÜNTÜ

Deepfake mi? Nasıl Anlaşılır?



Aceleye Getirme

Hızlı karar vermeye zorlayan mesajlara dikkat edin.



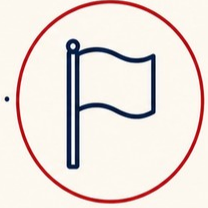
Bilgi Talebini Sorgula

Şifre, kod veya kişisel bilgi talebi ciddi bir uyarı işaretidir.



Kimliğini Doğrula

Başka bir kanaldan gerçekten o kişi olup olmadığını kontrol edin.



Bildir ve Yardım İste

Şüpheli içeriği bildirin, bir yetişkinden destek alın.

HIZLI KONTROL • Şüpheleniyorsanız asla bilgi paylaşmayın

Bu dört adımı çocuğunuzla birlikte bir kez gözden geçirmek, benzer bir durumla karşılaştığınızda ne yapması gerektiğini önceden bilmesini sağlar.

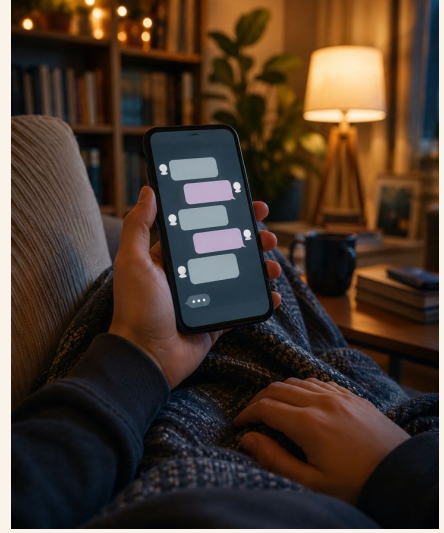
Deepfake teknolojisi sürekli geliştiği için hiçbir kontrol yöntemi yüzde yüz garanti vermez. Şüphe duyulan bir ses veya görüntü paylaşılmadan, harekete geçilmeden önce mutlaka başka bir kanaldan doğrulanmalıdır. Emin olunamayan durumlarda en güvenli tercih, bilgiyi yaymak yerine bir yetişkinle ya da okulun rehberlik servisiyle paylaşmaktır.

YAPAY ZEKA SOHBET BOTLARI

Yapay Zeka Sohbet Botları ve Sahte Samimiyet

Eskiden çocuklar internette yalnızca gerçek insanlarla sohbet ediyordu. Bugün ise birçok uygulamada karşılarına çıkan ilk “arkadaş”, aslında yapay zeka olabiliyor. Snapchat'teki My AI, Instagram ve benzeri uygulamalara eklenen yapay zeka özellikleri artık ayrı bir uygulama gerektirmeden doğrudan sohbet listesinde veya kamera ekranında yer alıyor.

Yapay zeka sohbet botları, kullanıcıyla doğal bir iletişim kurmak üzere tasarlanıyor. Çocuklar zamanla karşısındaki sistemin bir yazılım olduğunu unutup onu gerçek bir arkadaş, sırdaş veya kendisini her zaman anlayan biri gibi görebiliyor.



Risk, yapay zekanın kötü niyetli olmasından değil, kurulan bu sahte samimiyet hissinden kaynaklanıyor. Sohbet botları çoğunlukla kullanıcıyı onaylayan ve konuşmayı sürdürmeye odaklanan bir yapı sergiliyor, bu da bazı çocukların gerçek sosyal ilişkilerden uzaklaşmasına neden olabiliyor.

Bu riskler nedeniyle ABD'de Federal Ticaret Komisyonu (FTC), yapay zeka sohbet botlarının çocuklar üzerindeki etkisini incelemek üzere şirketlerden bilgi talep etti.

Biliyor muydunuz?

- Yapay zeka sohbet botlarıyla yapılan konuşmalar, hizmeti geliştirmek amacıyla kaydedilebilir ve analiz edilebilir.
- Yapay zekaya da gerçek bir insana söylemeyeceğiniz kişisel bilgileri paylaşmamalısınız.
- Çocuklar için yapay zeka, bir arkadaşın yerine geçmemeli. Bilgi edinmek ve öğrenmek için kullanılan bir araç olarak görülmelidir.

YAPAY ZEKA SOHBET BOTLARI

Gerçek Vaka: Bir Sohbet Botuyla Derinleşen Duygusal Bağ

Ne Oldu?

ABD'de 14 yaşındaki Sewell Setzer III, Character.AI platformundaki bir sohbet botuyla aylar boyunca yoğun bir duygusal ilişki kurdu. Ailesinin daha sonra açtığı davaya göre çocuk zamanla gerçek yaşamdan uzaklaştı, botu güvenilir ve romantik bir ilişki ortağı gibi algıladı ve ruhsal sıkıntılarını bu sohbetlerde dile getirdi.

Dava dosyasına göre sistem, riskli konuşmalar sırasında sohbeti sonlandırıp çocuğu bir yetişkine veya profesyonel desteğe yönlendirmekte yetersiz kaldı. Sewell, Şubat 2024'te yaşamını yitirdi. Ailesinin Character.AI ve Google'a karşı açtığı dava Ocak 2026'da bir uzlaşmayla sonuçlandı, uzlaşmanın koşulları açıklanmadı ve şirketlerin hukuki sorumluluğuna ilişkin kesinleşmiş bir mahkeme kararı verilmedi (kaynak: Reuters ve CNN Business haberleri, Ocak 2026).

Bu örnek istisnai bir uç durum. Ama gösterdiği şey açık: bir çocuğun yapay zekayla kurduğu ilişki, fark edilmeden derinleşebiliyor. Konuşmayı sürdüren, hiç itiraz etmeyen ve her zaman ulaşılabilir olan bir sohbet ortağı, gerçek destek ihtiyacının gözden kaçmasına neden olabiliyor.

Acil bir güvenlik veya kendine zarar riski varsa 112 aranmalı. Süreklilik gösteren duygusal sorunlarda çocuk ve ergen ruh sağlığı uzmanından destek alınmalı. Genel sosyal destek ve yönlendirme için Alo 183 Sosyal Destek Hattı da aranabilir.

Ailelerin yapabileceği en önemli şey, çocuklarının kullandığı uygulamalarda yapay zeka özelliklerinin bulunduğunu bilmek ve bu sistemlerin gerçek bir arkadaş olmadığını açıkça konuşmaktır.

ZORBALIK VE YAŞ SINIRI

Sosyal Medyada Zorbalık



Siber zorbalık yalnızca kötü bir yorum yazmak değildir. Bir çocuğu grup sohbetinden bilerek dışlamak, hakkında sahte hesap açmak, fotoğrafını izinsiz paylaşmak, özel mesajların ekran görüntülerini yaymak, topluca alay etmek veya oyun içinde sürekli hedef almak da zorbalığın farklı biçimleridir.

Dijital ortamda yapılan zorbalık okuldan çıktıktan sonra da devam edebilir. İçerik hızla yayılabilir, tekrar tekrar paylaşılabilir ve çocuk kendisini günün hiçbir saatinde güvende hissetmeyebilir.

Bu süreklilik, çevrim içi zorbalığın etkisini yüz yüze yaşanan tek bir olaydan daha ağır hale getirebilir.

Zorbalıkta yalnızca mağdur ve zorba yoktur. Mesajı paylaşan, gülen emoji bırakan, olayı izleyip hiçbir şey söylemeyen veya başkalarını gruba çağıran seyirciler de olayın büyümesine katkıda bulunabilir. Bu nedenle çocuklara yalnızca “zorbalık yapma” değil, gördükleri zorbalığa katılmama ve güvenilir bir yetişkine haber verme sorumluluğu da anlatılmalıdır.

Çocuklar yaşadıkları olayı çoğu zaman hemen anlatmaz. Telefonlarının alınacağından, suçlanacaklarından, arkadaşlarını kaybedeceklerinden veya olayın büyüyeceğinden korkabilirler. Bu nedenle ailelerin ve öğretmenlerin vereceği ilk tepki belirleyicidir.

Siber Zorbalığın Yaygın Biçimleri

- Grup sohbetinden dışlama veya gruba tekrar tekrar ekleyip çıkarma
- Fotoğraf, video ya da özel konuşmaları izinsiz yayma
- Sahte hesap açma veya başkasının hesabını taklit etme
- Toplu yorum saldırısı, alay ve hakaret
- Dedikodu, ifşa ve küçük düşürücü içerik üretme
- Oyun içinde kasıtlı dışlama, tehdit veya sürekli hedef alma
- Sessiz kalması için tehdit etme veya şantaj uygulama

Bir Çocuk Zorbalık Yaşadığını Anlatırsa

- Önce sakın biçimde dinlenmeli ve yaşananlardan dolayı suçlanmamalı.
- Mesajlar, kullanıcı adları, tarih ve saat bilgileri silinmeden ekran görüntüsüyle saklanmalı.
- İçerik platforma bildirilmeli, gerekli hesaplar engellenmeli.
- Okulla bağlantılıysa rehberlik servisi ve okul yönetimi bilgilendirilmeli.
- Tehdit, şantaj, taciz veya fiziksel tehlike varsa yetkili makamlara başvurulmalı.
- Çocuğun uyku, okul, arkadaşlık ve duygu durumundaki değişimler izlenmeli.

En Önemli Mesaj

- Çocuk, yaşadıklarını anlattığında telefonunun elinden alınmayacağını ve suçlanmayacağını bilirse yardım istemesi kolaylaşır.

Dünyada Yaş Sınırı Tartışması

Siber zorbalığın yaygınlığı, dünya genelinde sosyal medyada yaş sınırı tartışmasını da hızlandırdı. Avustralya, 10 Aralık 2025'te yürürlüğe giren bir düzenlemeyle, yaş sınırlı sosyal medya platformlarına 16 yaşından küçüklerin hesap sahibi olmasını önlemek için makul tedbirler alma yükümlülüğü getiren dünyanın ilk ülkesi oldu. Çocuklara veya ailelerine doğrudan bir yaptırım uygulanmıyor, yükümlülük ve olası cezalar platformlara ait. Düzenlemenin ilk ayında 4,7 milyondan fazla hesap kapatıldı ya da kısıtlandı. Ancak eSafety Commissioner'ın Temmuz 2026'da yayımladığı takip raporuna göre, düzenlemenin üçüncü ayında Avustralyalı çocukların yüzde 80'inden fazlası hala yaş sınırlı platformlara erişebiliyor, hesap sahipliği yüzde 52'den yüzde 42'ye gerilemesine rağmen günlük kullanım oranı neredeyse değişmedi (kaynak: eSafety Commissioner, Temmuz 2026).

Siber zorbalığa uğrayan gençlerin önemli bir bölümü yaşadıklarını okulda bir yetişkinle paylaşıyor. ABD'de yapılan 2025 araştırmasına göre mağdurların yüzde 66'sı durumu ebeveynine, yalnızca yüzde 31'i bir eğitmeniye bildirdi.

CYBERBULLYING RESEARCH CENTER, 2025 ARAŞTIRMASI (ABD)

MESAJLAŞMA

Özel Mesajlar ve Grup Sohbetlerindeki Riskler

Çocukların dijital iletişimi yalnızca mesajlaşma uygulamalarında gerçekleşmiyor. Sosyal medya özel mesajları, video platformlarının yorum alanları, oyun içi sohbetler, sınıf grupları ve geçici mesaj özellikleri de çocukların tanıdıkları veya tanımadıkları kişilerle iletişim kurduğu alanlara dönüşebiliyor.



Riskli bir iletişim çoğu zaman açıkça tehdit edici başlamaz. Karşıdaki kişi önce ortak ilgi alanlarından konuşabilir, çocuğun güvenini kazanmaya çalışabilir ve ardından sohbetin daha özel bir kanala taşınmasını isteyebilir.

“Burada konuşmayalım”, “mesajları sil”, “ailene söyleme” veya “sadece ikimizin arasında kalsın” gibi ifadeler önemli uyarı işaretleridir.

Özel mesajlarda karşılaşılabilecek riskler yalnızca yetişkinlerin çocuklara uygunsuz yaklaşımıyla sınırlı değildir. Arkadaş gruplarında dışlama, alay etme, özel konuşmaların ekran görüntüsünü paylaşma, sahte hesapla takip etme, oyun parası veya hediye kodu vaadiyle şifre isteme, konum ve fotoğraf talep etme gibi durumlar da sık görülen riskler arasındadır.

NCMEC'in (Ulusal Kayıp ve İstismara Uğramış Çocuklar Merkezi) verilerine göre, ABD'de finansal çevrimiçi şantaj bildirimleri 2024'te 36.000'in üzerindeyken 2025'te 50.000'in üzerine çıktı. NCMEC, saldırganların tespit edilmeyi zorlaştırmak için konuşmaları giderek daha hızlı özel mesajlaşmaya ve şifreli uygulamalara taşıdığını da belirtiyor.

Konuşmanın kaybolan mesaj özelliğine taşınması veya uçtan uca şifreli başka bir uygulamaya geçirilmek istenmesi, tek başına kötü niyetin kanıtı değildir. Ancak çocuğun konuşmayı gizlemesinin istenmesi, baskı kurulması veya kişisel bilgi talep edilmesiyle birleştiğinde ciddiye alınmalıdır.

Kırmızı Bayraklar

- Tanımadığı bir kişi kısa sürede aşırı samimi davranıyorsa
- Konuşmayı başka bir uygulamaya taşımak veya mesajları silmek istiyorsa
- Fotoğraf, canlı görüntü, konum, okul adı, telefon numarası veya şifre talep ediyorsa

- Hediye kodu, oyun parası, ücretsiz üyelik veya para vaat ediyorsa
- “Bunu aileme söylerim” ya da “bana cevap vermezsen paylaşırım” gibi baskı kuruyorsa
- Çocuęu arkadaşlarından veya ailesinden sır saklamaya yönlendiriyorsa

Mesaj Geldiğinde Üç Soru

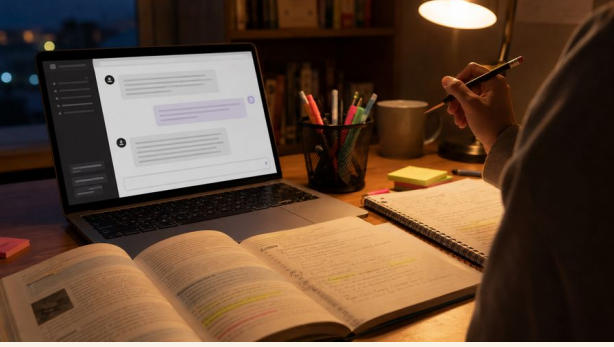
- Bu kişiyi gerçek hayatta tanıyor muyum?
- Neden konuşmayı gizlememi veya başka bir uygulamaya geçmemi istiyor?
- Benden kişisel bilgi, fotoğraf, konum, para ya da şifre istiyor mu?

Aileler Nasıl Yaklaşmalı?

Çocuęun bir mesajı göstermesi halinde ilk tepkinin öfke, yasak veya telefonu elinden alma olması, bir sonraki olayı saklamasına neden olabilir. Önce dinlemek, mesajları silmeden kanıtları saklamak, hesabı engellemek ve platforma bildirmek daha doğru bir sıralamadır. Tehdit, şantaj, cinsel içerik talebi veya fiziksel buluşma baskısı varsa okul yönetimi, rehberlik servisi ve gerekli durumlarda kolluk birimleriyle iletişime geçilmelidir.

YAPAY ZEKA VE ÖDEVLER

Yapay Zeka ile Hazırlanan Ödevler ve Bilgi Kirliliği



Yapay zeka araçları öğrencilerin bilgiye ulaşma, soru sorma ve çalışma yöntemlerini hızla değiştiriyor. Bir konuyu farklı örneklerle açıklamak, çalışma planı hazırlamak veya yazılmış bir metindeki anlatım sorunlarını görmek için kullanıldığında bu araçlar öğrenmeyi destekleyebilir.

Ancak yapay zekanın sunduğu cevaplar her zaman doğru, güncel veya güvenilir değildir. Bu sistemler bir cevabı oluştururken yalnızca doğrulanmış kaynakları sıralamaz.

Bazen eksik bilgileri birbirine bağlayarak gerçekte bulunmayan kitaplar, makaleler, kişiler veya tarihsel olaylar üretebilir. Üstelik bu yanlış bilgiyi tereddüt göstermeden, oldukça ikna edici bir dille sunabilir. Bu nedenle düzgün yazılmış bir cevap, doğru cevap anlamına gelmez.

Sorun yalnızca ödevi yapay zekaya yazdırmak değildir. Öğrencinin yapay zeka tarafından hazırlanan metni kendi cümleleriyle açıklayamaması, konuyu gerçekten öğrenmediğini gösterir. Kısa vadede zaman kazandıran bu yöntem, uzun vadede araştırma, düşünme, karşılaştırma ve yazma becerilerinin gelişmesini engelleyebilir.

Bir başka risk ise gizlilik. Öğrenciler ve öğretmenler, kişisel bilgileri, sınıf listelerini, sınav sorularını, başka öğrencilere ait çalışmalarını veya henüz yayımlanmamış okul belgelerini herkese açık yapay zeka sistemlerine yüklememelidir. Bu içerikler hizmetin çalışma biçimine göre kaydedilebilir, analiz edilebilir veya sistemlerin geliştirilmesinde kullanılabilir.

Yapay Zekadan Alınan Bilgi Nasıl Kontrol Edilir?

- Kaynak gerçekten var mı? Verilen kitap, makale, kurum veya internet sayfası ayrıca aranmalı.
- Aynı bilgi ders kitabında, resmi bir kurumun sitesinde veya güvenilir başka kaynaklarda geçiyor mu?
- Tarih, isim ve sayılar birbiriyle tutarlı mı?
- Öğrenci cevabı kendi cümleleriyle açıklayabiliyor mu?

- Yapay zekadan alınan metin, doğrudan teslim edilmek yerine yeniden düşünülüp düzenlenmiş mi?

Üç Soruluk Hızlı Kontrol

- Bu bilgi nereden geliyor?
- Başka bir güvenilir kaynak aynı şeyi söylüyor mu?
- Ben bu cevabı kendi cümlelerimle açıklayabiliyor muyum?

Veliler için

- Çocukla yalnızca “yapay zeka kullanma” üzerinden konuşmak yerine, hangi amaçlarla ve hangi sınırlar içinde kullanılabileceği birlikte belirlenebilir.
- Çocuğun ödevi nasıl hazırladığını anlatması, kullandığı kaynakları göstermesi ve yapay zekadan aldığı bilgiyi doğrulaması istenebilir.
- Amaç yakalamak veya cezalandırmak değil, öğrenme sürecini görünür hale getirmektir.

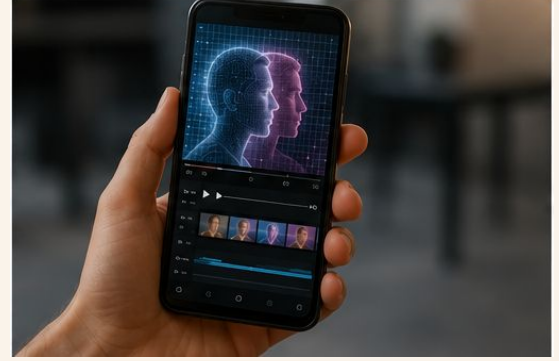
Öğretmenler için

- Ödevlerde yapay zeka kullanımına ilişkin sınırların baştan açıklanması belirsizliği azaltır.
- Öğrenciden kullandığı araçları, kaynaklarını ve hangi bölümde yapay zekadan destek aldığını açıklaması istenebilir.
- Yalnızca teslim edilen metnin değil, taslakların ve öğrencinin konuyu sözlü açıklayabilmesinin de değerlendirilmesi daha sağlıklı bir sonuç verir.

VIDEO GERÇEKLİĞİ

İnternette Görülen Videoların Doğruluğu

Çocuklar ve ergenler haberleri, gündelik olayları ve dünyadaki gelişmeleri giderek daha fazla kısa videolar üzerinden takip ediyor. Ancak bir videoda gerçek görüntüler bulunması, videonun anlattığı hikayenin doğru olduğu anlamına gelmez.



Yanıltıcı içerik farklı şekillerde üretilebilir. Eski bir görüntü yeni bir olaymış gibi paylaşılabilir. Başka bir kişiye ait ses videoya eklenebilir.

Görüntünün yalnızca belirli bir bölümü gösterilerek olayın bağlamı değiştirilebilir. Yapay zeka ile yüz, ses veya arka plan üretilebilir. Sahte altyazı, başlık ya da ekran görüntüsü eklenerek izleyicide yanlış bir izlenim oluşturulabilir.

Bu içerikler çoğunlukla güçlü bir duygu yaratmaya çalışır. Korku, öfke, şaşkınlık veya merak ne kadar yüksekse, kişinin videoyu kontrol etmeden paylaşma ihtimali de o kadar artar. “Hemen paylaş”, “bunu sizden saklıyorlar” veya “medya bunu göstermiyor” gibi ifadeler, izleyiciyi düşünmeden tepki vermeye yönlerebilir.

Bir videonun milyonlarca kez izlenmiş olması, çok sayıda yorum alması veya tanınmış bir hesap tarafından paylaşılması güvenilir olduğunu kanıtlamaz. Popülerlik, doğruluk göstergesi değildir.

Gerçek Vaka: Çocuklara Önerilen Yapay Zeka Videoları

Nisan 2026'da 200'den fazla çocuk gelişimi uzmanı, eğitimci ve kuruluş, YouTube'a çocuklara önerilen düşük kaliteli yapay zeka videolarıyla ilgili önlem alma çağrısı yaptı. Uzmanlara göre hızlı, renkli ve dikkat çekici bu videolar çocukların gerçek ile yapay olanı ayırt etmesini zorlaştırabiliyor.

Bir videonun çocuklara yönelik hazırlanmış veya çok izlenmiş olması, güvenilir ve gelişimlerine uygun olduğu anlamına gelmiyor.

(Kaynak: AP News, Nisan 2026)

VIDEO GERÇEKLİĞİ

Beş Adımda Doğrulama

1

Durun

Video güçlü bir duygu yaratıyorsa hemen paylaşmayın.

2

Kaynağa Bakın

Hesabın kim tarafından yönetildiği, ne zaman açıldığı ve daha önce ne paylaştığı incelenmeli.

3

Başka Kaynak Arayın

Aynı olay güvenilir haber kuruluşlarında veya resmi kurum hesaplarında yer alıyor mu?

4

Ayrıntıları Kontrol Edin

Tarih, hava durumu, tabela, kıyafet, dil ve konum birbiriyle uyumlu mu?

5

Şüphedeyseniz Paylaşmayın

Yanlış bilginin yayılmasını durdurmak, ilk paylaşan olmaktan daha değerlidir.

Veli ve Öğretmenler İçin Uygulama

- Çocuğa yalnızca “internette gördüğüne inanma” demek yerine, haftada bir şüpheli videoyu birlikte incelemek daha öğreticidir.
- Kaynağı bulmak, farklı haberleri karşılaştırmak ve görüntünün tarihini araştırmak eleştirel düşünme alışkanlığını geliştirir.

Yapay Zeka İzi Her Zaman Görünür Değildir

Yapay zeka ile üretilen içeriklerde bozuk el, uyumsuz dudak hareketi veya yapay ses gibi işaretler bulunabilir. Ancak teknoloji geliştikçe bu ipuçları daha az belirgin hale geliyor. Bu nedenle yalnızca görüntüde hata aramak yeterli değildir. En güvenilir yöntem, videonun kaynağını ve bağlamını doğrulamaktır.

EKRAN SÜRESİ

Ekran Süresi ve Kullanım Biçimi



Ekran süresi konusunda yalnızca saate bakmak yeterli değildir. Aynı süre içinde çevrim içi ders izlemek, arkadaşlarla konuşmak, yaratıcı bir çalışma yapmak veya kısa videoları aralıksız kaydırmak çocuk üzerinde aynı etkiyi yaratmaz.

Bu nedenle ailelerin “ne kadar?” sorusunun yanında “ne yapıyor, ne zaman kullanıyor ve kullanım sonrasında nasıl hissediyor?” sorularını da sorması gerekir.

Özellikle gece kullanımı, uyku saatini erteleyebilir ve bildirimler çocuğun zihinsel olarak çevrim içi kalmasına neden olabilir. Ders çalışırken telefonun sürekli görüş alanında olması da kullanılsa bile dikkati bölebilir. Yemek sırasında, yatmadan hemen önce veya aile içi iletişim zamanlarında ekran kullanımı arttıkça günlük denge bozulabilir.

Sosyal medyada pasif kullanım, yani uzun süre yalnızca başkalarının paylaşımlarını izlemek ve kaydırmak, karşılaştırma duygusunu artırabilir. Özellikle düzenlenmiş görüntüler, başarı hikayeleri ve kusursuz yaşam sunumları çocukların kendi hayatlarını yetersiz görmesine yol açabilir. Buna karşılık arkadaşla iletişim kurma, bir beceri öğrenme veya içerik üretme gibi amaçlı kullanım daha farklı bir deneyim yaratabilir.

Kuralların yalnızca çocuğa uygulanması çoğu zaman direnç doğurur. Yetişkinlerin yemek sırasında telefonu bırakması, yatak odasında ekran kullanmaması ve bildirimleri sınırlaması, söylenen kurallardan daha etkili bir örnek oluşturur.

EKRAN SÜRESİ

Aynı Süre, Farklı Etki

Öğrenmeyi ve İletişimi Destekleyen

- Canlı ders veya araştırma yapmak
- Arkadaşlarla mesajlaşmak
- Müzik, çizim veya video üretmek

Dengeyi Bozabilen

- Kısa videoları amaçsızca kaydırmak
- Gece geç saatlere kadar bildirim takip etmek
- Oyunu kontrolsüz biçimde uzatmak

Evde Uygulanabilecek Dengeli Kurallar

- Yemek sırasında ve yatmadan önce belirli bir süre ekran kullanılmaması
- Telefonların gece yatak odası dışında şarj edilmesi
- Ödev sırasında bildirimlerin kapatılması veya telefonun başka bir yerde tutulması
- Ekran süresinin bir anda yasaklanması yerine birlikte planlanması
- Haftalık olarak hangi içeriklerin iyi veya kötü hissettirdiğinin konuşulması
- Kuralların yalnızca çocuk için değil, ailedeki herkes için geçerli olması

Süre Kadar Şu Üç Soru da Önemlidir

- Ekranda ne yapıyor?
- Ekranı ne zaman kullanıyor?
- Kullanım sonrasında nasıl hissediyor?

Yaşa Göre Sınırlar

Küçük çocuklarda ekran süresi için yaşa göre daha net sınırlar önerilir. Aile ve Sosyal Hizmetler Bakanlığının Şubat 2026 tarihli ekran süresi uyarısında, 3 yaş için günde en fazla 30 dakika, 4 yaş için 40 dakika, 5 yaş için 50 dakika ve 6 yaş için 60 dakika önerilmektedir. Daha büyük çocuklarda ise tek bir süre sınırından çok uyku, okul, hareket, aile ilişkileri ve kullanılan içeriğin niteliği birlikte değerlendirilmelidir.

FARK ETME REHBERİ

Fark Etme Rehberi

Bir çocuk yaşadığı sorunu çoğu zaman önce davranışlarıyla gösterir. Tek bir belirti her zaman sorun anlamına gelmez, ancak birkaç belirti birlikte ve sürekli görülüyorsa konuşmayı başlatmak için iyi bir sebeptir.



Sahte Samimiyet ve Yoğun Dijital Kullanım

- Telefonunu daha çok saklıyor, biri yaklaşıncaya ekranı kapatıyor.
- Gerçek arkadaşlarına ayırdığı zaman azalıyor, yalnız kalmayı seçiyor.

İlk işaret çoğu zaman gizleme ve içine kapanmadır.



Zorbalık ve Ekran Süresi

- Bildirim geldiğinde huzursuzlanıyor, telefonu aniden kapatıyor.
- Uyku düzeni bozuluyor, geç saatlere kadar çevrim içi kalıyor.

Aniden değişen ruh hali ve uyku düzeni önemlidir.



Mesajlaşma Riskleri

- Tanımadığı biriyle konuşurken başka uygulamaya geçmek istiyor.
- Kaynağı belirsiz hediye, para veya özel mesajlar dikkat çekiyor.

Gizli konuşma talebi önemli bir uyarı işaretidir.



Ödev ve Bilgi Güvenilirliği

- Ödevini nasıl hazırladığını veya kaynaklarını açıklayamıyor.
- Yapay zekadan aldığı bilgiyi sorgulamadan doğru kabul ediyor.

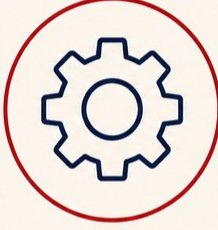
Cevabı kendi cümleleriyle açıklayamaması dikkat çekebilir.

Tek bir belirti her zaman sorun anlamına gelmez. Ama birkaç belirti birlikte ve sürekli görülüyorsa sakın bir konuşma başlatmak için iyi bir sebeptir.

KORUNMA

AİLE İÇİN UYARI

Güvenli Dijital Kullanım İçin Üç Temel Adım



Ayarları Gözden Geçirin

Yapay zeka özelliği var mı, kimler mesaj gönderebiliyor kontrol edin.



Açık İletişimi Sürdürün

Çocuğunuz cezalandırılmayacağını bilsin, bu en güçlü koruma.



Kuralları Aile Olarak Belirleyin

Ekransız saatler tüm aileye uygulandığında daha kalıcı olur.

AİLE İÇİN

- Kuralları birlikte belirleyin, birlikte uygulayın

Bu üç adımı bir defada değil, zaman içinde küçük konuşmalarla ele almak genellikle daha kalıcı sonuç verir.

Aile İçin Kontrol Notu

- Ayarların gözden geçirilmesi tek seferlik bir iş değildir, uygulamalar güncellendikçe yeniden kontrol edilmesi gerekir.
- Ekransız saatleri, paylaşılmayacak bilgileri ve yapay zekanın hangi amaçlarla kullanılabileceğini birlikte belirleyin.
- Aile içinde belirlenen kuralların herkes için geçerli olması, çocuğun bu kuralları adil bulmasını kolaylaştırır.

BİR ŞEY TERS GİDERSE

İzlenecek Müdahale Akışı

**Dinle**

Sakin kalın, çocuğunuzu suçlamadan dinleyin.

**Kanıtı Sakla**

Şüpheli mesaj veya görüntünün ekran görüntüsünü alın.

**Hesabı Güvene Al**

Hesap şifrelerini değiştirin, diğer hesapları da güncelleyin.

**Bildir**

İçeriği platforma bildirin.

**Yetkiliye Başvur**

Gerekirse okul veya emniyetle iletişime geçin.

**Destek Al**

Bir uzmandan destek almaktan çekinmeyin.

KAYIT VE BİLDİRİM • Kanıtları saklayın, bildirimini geciktirmeyin

Bu akışı bir kez birlikte okumak, gerçek bir durumla karşılaşıldığında panik yapmadan hareket etmeyi kolaylaştırır.

Acil Durumda

- Kendine zarar verme riski, tehdit içeren bir mesaj ya da fiziksel bir tehlike söz konusuysa vakit kaybetmeden 112 aranmalı.
- Süreklilik gösteren duygusal sorunlarda çocuk ve ergen ruh sağlığı uzmanından destek alınmalı.
- Hesap ele geçirilmişse önce kanıt saklanmalı, şifre bundan sonra değiştirilmeli, aksi halde bazı deliller kaybolabilir.

Çocuklarınız İçin Daha Güvenli Bir Dijital Yaşam

Okullara ve kurumlara yönelik dijital güvenlik farkındalık eğitimleri için bizimle iletişime geçebilirsiniz.

Sparta Siber Güvenlik Teknolojileri · 0 312 909 33 02
www.sparta.com.tr · sparta@sparta.com.tr

BAŞLICA KAYNAKLAR

TÜİK, Çocuklarda Bilişim Teknolojileri Kullanım Araştırması, 2024.

TÜİK, Hanehalkı Bilişim Teknolojileri Kullanım Araştırması, 2025.

TBMM Çocukların Suça Sürüklenmesine Yol Açan Nedenlerin Araştırılması Komisyonu tutanakları (Başkan Müşerref Pervin Tuba Durgut), 2026.

TBMM Şanlıurfa ve Kahramanmaraş'ta Okullarda Meydana Gelen Olaylar ile Çocukların Dijital Ortamlarda Karşılaştıkları Riskler Araştırma Komisyonu tutanakları (Başkan Yusuf Beyazıt), 24-25 Haziran 2026.

UNESCO, Eğitim ve Araştırmada Üretken Yapay Zeka Rehberi.

Ofcom, Children and Parents: Media Use and Attitudes Report, 2026.

World Economic Forum, "Real-time deepfakes are rewriting the rules of child safety", Nisan 2026.

eSafety Commissioner (Avustralya), sosyal medya yaş sınırı yasası üç aylık takip raporu, Temmuz 2026.

Cyberbullying Research Center (Patchin ve Hinduja), siber zorbalık bildirim oranları araştırması, 2025 (ABD).

FBI, çocuklara yönelik çevrimiçi yaklaşımların gerçekleştiği ortamlara ilişkin değerlendirme (ABD).

NCMEC (National Center for Missing & Exploited Children), finansal çevrimiçi şantaj (sextortion) verileri, 2025 (ABD).

NSPCC, özel mesajlaşmada çevrimiçi istismarla mücadele raporu, Kasım 2025 (İngiltere).

Fairplay ve 200'den fazla uzman ile kuruluşun YouTube'a çağırısı, AP News haberleri, Nisan 2026 (ABD).

Reuters ve CNN Business, Character.AI ve Google'a karşı açılan dava haberleri, Ocak 2026.

T.C. Aile ve Sosyal Hizmetler Bakanlığı, "Çocuklar Güvende" internet sitesi, ekran süresi uyarısı, Şubat 2026.

Yasal Uyarı

Bu dokümanda yer alan bilgiler genel bilgilendirme ve farkındalık amacıyla hazırlanmıştır ve siber güvenlik danışmanlığı kapsamında değildir. İçerik, güvenilir olduğu değerlendirilen kaynaklardan derlenmiştir, ancak Sparta Siber Güvenlik Teknolojileri Ltd. Şti. bu bilgilerin eksiksizliği veya doğruluğu konusunda garanti vermez ve kullanımından doğabilecek zararlardan sorumlu tutulamaz.

Doküman ticari amaç gözetilmeksizin kişisel bilgilendirme için kullanılabilir, indirilebilir ve paylaşılabılır, ancak kaynağın Sparta Siber Güvenlik Teknolojileri Ltd. Şti. olduğu belirtilmelidir. Önceden yazılı izin alınmadan doküman içeriği ticari amaçla çoğaltılamaz veya yeniden yayımlanamaz.