

Gizlilik ve Güvenlik

<p>RİSK: Zayıf ve Tahmin Edilebilir Şifreler</p> <p>123456 gibi zayıf ve tahmin edilebilir şifreler saniyeler içinde kırılabilir ve hesapların çalınmasına yol açabilir.</p>	<p>İPUCU: Güçlü Koruma Kalkanları Oluşturun</p> <p>Uzun ve karmaşık şifreler kullanın, her hesap için farklı bir şifre belirleyin ve İki Aşamalı Doğrulamayı (2FA) etkinleştirin.</p>
<p>RİSK: Kişisel Bilgilerin Paylaşılması</p> <p>Adres, okul, telefon numarası gibi bilgiler kötü niyetli kişiler tarafından kullanılabilir</p>	<p>İPUCU: Dijital Mahremiyet Bilinci Kazandırın</p> <p>Çocuğunuza özel bilgilerin internette tanımadığı kişilerle asla paylaşılmaması gerektiğini öğretin.</p>

Sosyal Medya

<p>RİSK: Kalıcı Dijital Ayak İzleri ve "Sharenting"</p> <p>İnternette paylaşılan her şey kalıcıdır ve gelecekte çocuğun karşısına çıkabilir. Ayrıca sharenting denilen ebeveynlerin paylaşımı da bir risktir.</p>	<p>İPUCU: Bilinçli Paylaşım ve Rol Model Olma</p> <p>Çocuğunuzun özel fotoğraflarını ve bilgilerini paylaşmaktan kaçının. Sosyal medya hesaplarında gizlilik ayarlarını birlikte yapın.</p>
<p>RİSK: Yanlış Bilgi ve Tık Tuzakları</p> <p>Sosyal medyada hızla yayılan yalan haberler (dezenformasyon) ve merak uyandıran başlıklar zararlı içeriklere yönlendirebilir.</p>	<p>İPUCU: Eleştirel Düşünmeyi Öğretin: Dur, Düşün, Paylaş!</p> <p>Karşılaştığı her bilgiyi sorgulamasını, kaynağını kontrol etmesini ve doğrulamadan paylaşmamasını telkin edin.</p>

Siber Zorbalık

<p>RİSK: Sanal Dünyanın Acımasız Yüzü</p> <p>Alay etme, dışlama, tehdit veya aşağılayıcı içerikleri yayınlama gibi davranışlar çocuklarda derin psikolojik yaralar açar.</p> <p>RİSK: Dijital Linç ve Sürü Psikolojisi</p>	<p>İPUCU: Sakin Kalın, Dinleyin ve Kanıt Toplayın</p> <p>Çocuğunuza güven verin, durumu anlatmasını sağlayın. Mesajların ekran görüntüsünü alın ve zorbalık yapan hesabı engelleyip şikâyet edin.</p> <p>İPUCU: Empatiyi Teşvik Edin</p>
<p>Olayın aslını bilmeden bir kişiye karşı toplu saldırılar, masum birinin bile büyük zarar görmesine neden olabilir.</p>	<p>"Bu sana yapılsaydı ne hissederdin?" sorusunu sorarak çocuğunuzu başkalarının yerine kendini koyma becerisini geliştirin.</p>

Yapay Zekâ (AI)

<p>RİSK: Aşırı Bağımlılık ve Düşünme Tembelliği</p> <p>Her kararı yapay zekaya sormak, çocukların eleştirel düşünme ve problem çözme yeteneklerini zayıflatır.</p>	<p>İPUCU: Yapay Zekâyı Karar Verici Değil, Araç Olarak Kullanın</p> <p>"Bot değil, beyin sensin" mottosuyla çocuğunuzu kendi fikirlerini oluşturmaya, yapay zekâdan aldığı bilgiyi başka kaynaklardan kontrol etmeye teşvik edin.</p>
<p>RİSK: Gizli Veri Toplama</p> <p>Yapay zekâyâ sorulan kişisel sorular ve kararlar sunucularda depolanır ve kötüye kullanılabilir.</p>	<p>İPUCU: Özel Bilgileri Yapay Zekâdan Uzak Tutun</p> <p>Çocuğunuza hassas kişisel bilgilerini ve özel sırlarını yapay zekâ sohbet robotlarıyla paylaşmaması gerektiğini öğretin.</p>

Dijital Oyunlar

<p>RİSK: Kontrolsüz Oyun İçi Harcamalar</p> <p>"Ganimet sandıkları" (lootbox) ve uygulama içi satın alımlar, farkında olmadan yüksek maliyetlere yol açabilir.</p>	<p>İPUCU: Ebeveyn Kontrolleri ve Aile Kuralları Belirleyin</p> <p>Cihazlardan oyun içi satın alımları kısıtlayın veya şifreye bağlayın. Harcama limitleri hakkında net kurallar koyun.</p>
<p>RİSK: Yabancılarla Sohbet ve Uygunsuz İçerik</p> <p>Oyun içi sohbetler siber zorbalığa, kötü niyetli yetişkinlerle temasa ve yaşa uygun olmayan konuşmalara zemin hazırlayabilir.</p>	<p>İPUCU: Yaş Sınırlarına Uyun ve Birlikte Oynayın</p> <p>Oyunların yaş derecelendirmelerini (PEGI vb) kontrol edin. Oyunu birlikte oynayarak hem içeriği denetleyin hem de çocuğunuzla iletişim kurun.</p>