

ÇOCUKLARIN KİŞİSEL VERİLERİ: EBEVEYNLER, PAYLAŞIM ve KORUMA

ÇOCUKLARA YÖNELİK KİTAPÇIK



Dr. Öğr. Üyesi Tülay KİTAPÇIOĞLU YÜKSEL

Dr. Öğr. Üyesi Cemile TURGUT

Klinik Psikolog Süreyyanur KİTAPÇIOĞLU

Bahadır POLAT

Berrin TAYMUR

ÇOCUKLARIN KİŞİSEL VERİLERİ: EBEVEYNLER, PAYLAŞIM ve KORUMA

ÇOCUKLARA YÖNELİK KİTAPÇIK

Bu kitapçık "223K804" numaralı, "Çocuğun Kişisel Verilerinin Ebeveyni Tarafından Sosyal Ağlarda Paylaşılmasının Psikolojik ve Hukuki Açıdan İncelenmesi" isimli TÜBİTAK projesi kapsamında hazırlanmıştır.

Dr. Öğr. Üyesi Tülay KİTAPÇIOĞLU YÜKSEL
Dr. Öğr. Üyesi Cemile TURGUT
Klinik Psikolog Süreyyanur KİTAPÇIOĞLU
Bahadır POLAT
Berrin TAYMUR

HAKKIMIZDA

Biz Kimiz?

Tülay Kitapçioğlu Yüksel : 2011 yılında Marmara Üniversitesi Hukuk Fakültesi'nden dördüncü olarak mezun olmuştur. 2014 yılında aynı üniversitede yüksek lisans tezini yüksek onur derecesiyle tamamlamış, 2021'de ise İstanbul Üniversitesi'nde doktora tezini başarıyla savunarak doktor unvanını almıştır. 2011'den itibaren avukatlık ve 2016 yılından itibaren de araştırma görevlisi olarak başladığı kariyerini, 2022'den bu yana Kırklareli Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı'nda Dr. Öğr. Üyesi olarak devam ettirmektedir. Ceza hukuku alanında akademik yayınlar yapmakta, bilimsel toplantılarda aktif rol almakta ve yurt dışında misafir araştırmacı olarak çalışmalar yürütmektedir. Tübitak projesinin yürütücülüğünü sürdürmektedir. Evli ve 2 çocuk annesidir.

Cemile Turgut : İstanbul Üniversitesi Hukuk Fakültesi'nden mezun olan Cemile Turgut, 2014 yılında İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı'nda yüksek lisansını tamamlamıştır. 2021 yılında İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı'nda "Kişilik Hakkının Bir Görünümü Olarak Unutulma Hakkı" isimli doktora tezini savunmuş, Doktor unvanını almıştır. Doktora sürecinde İngiltere ve İtalya'da misafir araştırmacı olarak çalışmalarını sürdürmüştür. 2014 tarihinde araştırma görevlisi olarak başladığı akademik hayatını, Koçeli Üniversitesi Hukuk Fakültesi Medeni Hukuk Anabilim Dalı'nda Dr. Öğretim Üyesi olarak devam ettirmektedir. Tübitak projesinde araştırmacı olarak görevini sürdürmektedir.

Süreyyanur Kitapçioğlu : İstanbul Üniversitesi Psikoloji Bölümü'nden 2015 yılında mezun oldu, Hasan Kalyoncu Üniversitesi'nde yüksek lisansını ergenlerde çevrimiçi oyun bağımlılığı üzerine tamamladı. Aynı üniversitede klinik psikoloji alanında doktora yapmaktadır ve tezini oyun bağımlılığı üzerine yazmaktadır. Özel bir danışmanlık merkezinde çocuklar, ergenler ve ailelerle çalışmakta; oyun ve teknoloji bağımlılığı konusunda eğitimler ve seminerler vermektedir. Yeşilay gönüllüsü olarak Türkiye Bağımlılıkla Mücadele çerçevesinde düzenlenen teknoloji bağımlılığı eğitimlerinde görev almaktadır. Tübitak projesinde araştırmacı olarak görevini sürdürmektedir.

Bahadır Polat : 2017 yılında Sakarya Üniversitesi Hukuk Fakültesi'nden mezun olmuştur. 2021 yılından bu yana Kırklareli Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalında araştırma görevlisi olarak görev yapmaktadır. Halihazırda Kırklareli Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Doktora programında öğrenimini sürdürmektedir. Tübitak projesinde bursiyer olarak görevini sürdürmektedir.

Berrin Taymur : 2019 yılında Uludağ Üniversitesi Hukuk Fakültesi'nden onur derecesiyle mezun olmuştur. 2020 yılında avukatlık ruhsatını alarak çeşitli hukuk bürolarında stajyer ve avukat olarak görev yapmıştır. 2022 yılından itibaren Kırklareli Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Yüksek Lisans programında eğitimine devam etmektedir. Tübitak projesinde bursiyer olarak görevini sürdürmektedir.

İÇİNDEKİLER



Hakkımızda	2
Amacımız.....	5
Neden Önemli?.....	6
Kişisel Veri Kavramı	7
Hukuki Riskler Nelerdir?	8
Kişisel Verileriniz = Kişiliğiniz.....	9
Sharenting Kavramı.....	10
Kişisel Verilerinizin Ebeveynleriniz Tarafından Sosyal Medyada Paylaşılması Haklarınızı İhlal Edebilir.....	12

Ebeveynlerinizin Bazı Paylaşımları	
Velayet Hakkı Kapsamında Olabilir.....	13
Mutlaka İzniniz Olmalı-İzin Yoksa Harekete Geçelim	14
Ebeveynlerin Paylaşımları ve Cezai Sorumlulukları.....	15
Ebeveyninizin Kişisel Verilerinizi Sosyal Ağlarda Paylaşması Hangi Hallerde Suç Teşkil Eder? - 1.....	16
Ebeveyninizin Kişisel Verilerinizi Sosyal Ağlarda Paylaşması Hangi Hallerde Suç Teşkil Eder? - 2.....	16
Ebeveynlerin Çocuklarının Kişisel Verilerini Paylaşmaları Halinde Olabilecek Suçlar Nelerdir?	17
Rızanız Varsa Suç Oluşmaz.....	18
Şikâyet Hakkınız Var Mı?.....	19



Dijital Açıdan Gizlilik ve Güvenlik Ayarları	20
Güçlü Şifreler ve İki Faktörlü Doğrulama	21
Güvenli İnternette Gezmek İster Misiniz?.....	23
Güncellemeler Sizi Güvende Tutar.....	24
Wi-Fi Ücretsiz Mi? Bedelini Siz Ödemeyin	25
Çerezler ve Dijital İzler	27
Uygulamalar ve Kişisel Veriler.....	29
Tanımadıklarımıza "Hayır" Deme Cesareti.....	30
Sanal Dünyada Güvenlik Testi	31
Teşekkürler.....	32



Amacımız

Bu kitapçık, çocukların kişisel verilerinin korunmasının önemini vurgulamak, ebeveynleri tarafından sosyal ağlarda paylaşıldığında doğabilecek risklere dikkat çekmek, kişisel verilerini ve haklarını nasıl koruyabilecekleri konusunda **çocukları** bilgilendirmek amacıyla hazırlanmıştır.

Neden Önemli?

Çocuğa ait görüntülerin, videoların ve bilgilerin sosyal ağlarda paylaşılması, hukuki ve psikolojik riskler doğurabilir. Bu riskleri bilmek ve önlem almak gerekmektedir. Ebeveynlerin çocuklarına ait kişisel verileri sık ve rıza dışı paylaşması, çocuğun kişilik hakkını ihlal eder ve velayet hakkının kötüye kullanımı sayılabilir. Bu durum hukuki ve cezai sorumluluk doğurabileceğinden farkındalık oluşturmak önemlidir. Ayrıca kontrolsüz paylaşımlar, çocukların psikolojik gelişimini olumsuz etkileyebilir, güven ilişkisini zedeleyebilir ve ilerleyen yıllarda sosyal kaygı, akran zorbalığı gibi sorunlara yol açabilir.



Kişisel Veri Kavramı

Kişisel Verilerimizin Farkında Olalım

Kişisel veri, sizi tanımamızı sağlayan her türlü bilgidir.

Örneğin, kişisel verileriniz şunlardır:

- İsmi ve soy ismi
- Doğum tarihiniz ve doğum yeriniz
- Fiziksel özellikleriniz
- Ailenizle ilgili bilgiler
- Telefon numaranız ve adresiniz
- Fotoğraflarınız ve ses kayıtlarınız
- Parmak iziniz ve sağlık bilgileriniz
- Şifreleriniz ve mesajlarınız



Hukuki Riskler Nelerdir?



Size ait görüntülerin, videoların, bilgilerin sosyal ağlarda paylaşılması birçok hukuki riski beraberinde getirir. Bu hukuki risklerin neler olduğu bilinmeli ve ona göre baştan önlem almak gerekmektedir.

Hukuki riskler şu şekildedir:

- **Veri ihlali:** Bilgiler, fotoğraflar, başkaları tarafından kopyalanabilir, çoğaltılabilir, kullanılabilir. Bilgilerin paylaşılması, sizin kişisel veriniz üzerindeki hakkınızı ihlal eder ve mahremiyetinize veya onur ve saygınlığınıza yönelik tehditlere ve saldırılara karşı sizi korumasız hale getirir.
- **Dijital kimlik hırsızlığı:** Başka kişiler, sizin bilgilerinizi ele geçirip kendi görüntülemiş gibi paylaşım kimliğinizi kullanabilirler.
- **Çocuğa ulaşma:** İsminizin, doğum tarihinizin, gittiğiniz okulun vb. görüntülerin paylaşılması, hatta sürekli nerede olduğunuza yönelik anlık konum etiketleri, kötü amaçlı kişilerin fiziki olarak size ulaşmasına neden olmaktadır.
- **Profil çizilmesi:** Verilerinizin/görüntünüzün farklı periyodik zamanlarda sosyal ağ platformlarına aktarılması size bir profil çizilmesine neden olmaktadır. Bu profil; hangi mal ve hizmetleri tüketmeye meyilli olduğunuza yahut olağan yaşam pratiklerinize, alışkanlıklarınıza yönelik şeffaf olmayan profillemeye riskini ve bu bilgilerin ise reklam, sigorta vb. şirketlere satılma tehlikesini beraberinde getirir.
- **Derin Sahtecilik (deep fake) riski:** Sosyal ağlarda paylaşılan bir fotoğraftaki yüz, rıza olmaksızın uygunsuz (müstehcen, suç içeren vb.) içerikte yer alan kişinin yüzüne monte edilebilmekte ve gerçekten yüzü monte edilen kişi o içerikteymiş hissi yaratılmaktadır.
- İleride unutulma hakkının öznesi haline gelebilirsiniz.
- Bu tehlike ve saldırılara yönelik hukuki imkânlar elbette ki mevcuttur. Fakat internet ortamında bir kere yayılmaya başlayan veri daha sonra kaldırılrsa dahi gerçek anlamda yok olmamaktadır. İmkânlar, internetin veriyi yayma gücü bağlamında yetersiz kalmaktadır.

Kişisel Verileriniz = Kişiliğiniz

Başkalarının kişisel bilgilerinizi kötü amaçlarla kullanmasını önlemenin en etkili yolu, onları korumaktır.

Fotoğrafınızın veya diğer bilgilerinizin izinsiz paylaşılmasını istememek en doğal hakkınızdır.

Kişisel bilgileriniz sizin kontrolünüzde olmalıdır.



Kontrolü kaybetmeyin, başkasına kaptırmayın.

Veriniz nasıl başkaları tarafından kullanılabilir?

İnternette gezerken bazen hangi bilgileri paylaştığınızı fark etmeyebilirsiniz. Ancak:

- Bilgileriniz, fotoğraflarınız başkaları tarafından kopyalanabilir, çoğaltılabilir, kullanılabilir.
- Bazı uygulamalar verilerinizi paylaşabilir. Oyunlar ve eğlence uygulamaları bile hakkınızda bilgi toplayabilir. Bu bilgiler başkalarına satılabilir, aktarılabilir.

Bu yüzden, hangi bilgileri paylaştığınızı, neye izin verdiğinizi her zaman kontrol etmelisiniz.





Sharenting (Paylaşanebeveynlik) Kavramı

Anne ve babanız hiç sizin fotoğraflarınızı sosyal medyada paylaştı mı? Doğum gününüz, parkta oynarken çekilen bir video veya okul başarınız...

Sharenting, anne ve babaların siz çocuklarla ilgili fotoğraf, video veya bilgileri sosyal medyada paylaşmasıdır. İngilizcedeki paylaşmak (*share*) ve ebeveynlik (*parenting*) kelimelerinin birleşiminden oluşmaktadır.

Neden Önemli?

-  **İnternet unutmaz** : Bir kez paylaşılan bilgi kolay kolay silinmez.
-  **Kimler görebilir?** : Paylaşımlar sadece aile bireyleriyle sınırlı kalmaz.
-  **Dijital ayak izi bırakır** : Gelecekte sosyal ve psikolojik gelişimi etkileyebilir.

Çocuklar Ne Düşünüyor?

Her 4 çocuktan 1'i, ebeveyninin paylaşım yapmadan önce izin almasını istiyor.

- Bazı çocuklar, internette kendileriyle ilgili paylaşımlardan utanıyor.

- “Acaba başkaları ne der?” kaygısı taşıyanlar var.
- **Özgüven eksikliği**: “Başkaları benim hakkımda ne düşünüyor?”
- **Kaygı**: “Kötü yorumlar gelirse ne olur?”

Ebeveynler Neden Paylaşır?

- Aile üyeleriyle anı paylaşmak
- Diğer ebeveynlerden tavsiye almak
- Eğlenceli anıları saklamak
- Beğeni ve yorum almak



Ancak, ebeveynler çocuklarının **dijital kimliğini şekillendirdiklerinin farkında olmayabilirler.**

Ne Yapabiliriz?

- **Ebeveynlerimizle konuşabiliriz:**
- “Bu fotoğrafı paylaşmadan önce bana sorar mısın?”
- “Bu fotoğraf özel, paylaşılmasını istemiyorum.”



Sharenting hakkında arkadaşlarınızla konuşun ve fikirlerinizi paylaşın.





Kişisel Verilerinizin Ebeveynleriniz Tarafından Sosyal Medyada Paylaşılması Haklarınızı İhlal Edebilir.

Aileniz sizinle ilgili her bilgiyi/görüntüyü paylaşamaz.

Herkesin **mahremiyet ve güvenlik hakkı** vardır. Mahremiyet, kişisel bilgilerinizi ve özel alanınızı korumanız anlamına gelir.

Mahremiyetinize ilişkin bazı görüntüler (**örneğin**, banyoda, tuvalette vb.) hiç paylaşılmamalıdır.

Bunun dışında evde veya özel anlarda çekilen fotoğraflar ise ancak sizin **İZNİNİZLE** paylaşılabilir.

Bazı paylaşımlar sizi ileride rahatsız edebilir, utanmanıza ya da **üzülmenize** neden olabilir.



Görüntülerinizin paylaşılmasını istemediğiniz her an **"HAYIR"** diyebilirsiniz.

- **Özel Alanınıza Saygı Gösterin:** Özel bilgilerinizi paylaşmaktan sakının.
- **Güvenli Olun:** Paylaşılan bilgiler kötü niyetli kişilerin eline geçebilir.
- **Mutlu Olun:** Bazen istemediğiniz bir fotoğraf ya da bilgi paylaşılsa üzgün hissedebilirsiniz.

Ebeveynlerinizin Bazı Paylaşımları Velayet Hakkı Kapsamında Olabilir.

Anne babaların 18 yaşından küçük siz çocuklar üzerinde velayet hakkı vardır. Ancak bu hak **sınırsız değildir** ve bazı yükümlülükleri içerir. Velayete ilişkin hak ve yükümlülüklerin temel amacı **sizlerin korunması** ve **menfaatinizin gözetilmesidir**.

Anne babanız tarafından yapılan ve sizi rahatsız, güvensiz, tedirgin hissettiren paylaşımlar menfaatinize aykırı olabilir ve velayet hakkının kötüye kullanılması teşkil edebilir.

Bunun haricinde aileniz bazen güzel ve iyi hissettiren anlarınızı paylaşmak isteyebilir. Paylaşım sizi rahatsız, tedirgin etmiyorsa ve güvenliyse ebeveyninizin velayet hakkı kapsamında olabilir. Ancak yine de sizin fikrinizin alınması ve izninizin olması önemlidir.

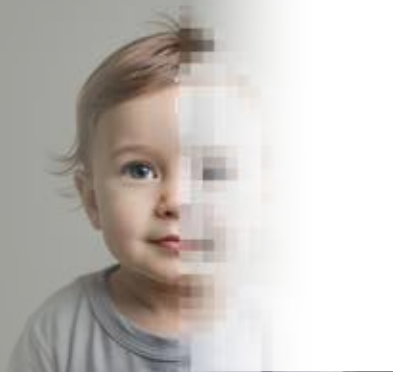
Bu paylaşımlar **sınırlı kişilerle** ve **güvenli** bir şekilde yapılmalıdır.

Kendinizi rahat hissetmiyor, tedirgin ve mutsuz hissediyorsanız her zaman paylaşımın kaldırılmasını ailenizden isteyebilirsiniz.

Aileniz sizi seviyor ve gelişiminizi önemsiyor. Paylaşımlar konusunda **açıkça konuşarak** hem güvenli hem rahat hissedebilirsiniz.



Mutlaka İzniniz Olmalı-İzin Yoksa Harekete Geçelim

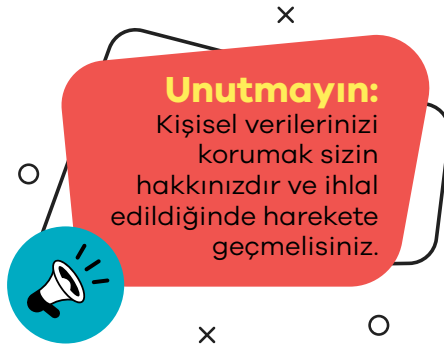


Ailenizden biri, öğretmeniniz veya en yakın arkadaşınız dahi olsa fotoğraflarınızı paylaşıırken **İZNİNİZİ almak zorundadır**. Bir şeye **“EVET”** demeden önce iyice düşünmelisiniz. Paylaşım yaparken veya bir şeye izin verirken dikkatli olmalısınız.

İzniniz dışında paylaşılan kişisel veriler için harekete geçmelisiniz. Eğer bir fotoğrafınız, videonuz ya da bilgileriniz izniniz olmadan paylaşılmışsa, bunların kaldırılmasını istemek en doğal hakkınızdır.

Ne Yapmalısınız?

- Ailenizden biri fotoğrafınızı veya videonuzu paylaştıysa ve bu sizi rahatsız ediyorsa, mutlaka onlara söylemelisiniz.
- *“Bir kere izin verdim, artık silemem”* diye düşünmemelisiniz. Kararınızı değiştirmek en doğal hakkınızdır.
- Önce paylaşan kişiyle iletişime geçerek, görselin veya bilginin kaldırılmasını isteyebilirsiniz.
- Eğer kaldırmazsa, bir büyüğünüzden yardım alabilirsiniz. Öğretmeniniz, aileniz veya okul rehberlik servisi size destek olabilir.
- *Facebook, Instagram, YouTube* gibi sosyal medya platformlarında *“Şikâyet Et”* seçeneğini kullanarak bilgilerinizi kaldırmalarını talep edebilirsiniz.
- Platform başvurunuzu reddederse, size verdiği cevap yetersizse veya 30 gün içinde başvuruza hiç cevap vermemişse Kişisel Verileri Koruma Kurulu’na şikâyet edebilirsiniz.



Ebeveynlerin Paylaşımları ve Cezai Sorumlulukları

Ebeveyniniz dahi olsa sizin **izniniz olmadan** kişisel verilerinizi paylaşamaz. Sizin özel hayatınızı ihlal eden, çocuk istismarı niteliğinde olan, psikolojik açıdan size rahatsızlık verebilecek, size zarar verebilecek paylaşımlar yapamaz. Eğer ebeveyniniz, izniniz olmadan bu tür paylaşımlar yapıyor ise bu hareketler, suç teşkil edebilir ve cezai sorumluluk doğurabilir.





Ebeveyninizin kişisel verilerinizi sosyal ağlarda paylaşması hangi hallerde suç teşkil eder? - 1

Eğer ebeveynlerinizin paylaşımları, fiziksel, psikolojik, cinsel gelişim açısından istismar niteliğinde ve herkes tarafından görülebiliyorsa suç teşkil eder.

Ebeveyninizin kişisel verilerinizi sosyal ağlarda paylaşması hangi hallerde suç teşkil eder? - 2



Eğer ebeveynleriniz, fotoğraf ve videolarınızı, günlük hayatın bir parçası haline getirerek paylaşıyor, bunu sıklıkla ve düzenli bir şekilde yapıyor veya rızanız dışında paylaşıyor ise ebeveynlerinizin cezai sorumluluğu gündeme gelir.

Ebeveynlerin Çocuklarının Kişisel Verilerini Paylaşmaları Halinde Oluşabilecek Suçlar Nelerdir?

Çocuklara ait kişisel verilerin hukuka aykırı şekilde yayımlanması ya da özel hayatının gizliliğinin ihlal edilmesi, Türk Ceza Kanunu'nda yer alan bazı suçları oluşturabilmektedir.

Bu suçlar şunlardır;



Özel hayatın gizliliğini ihlal
(TCK m.134)



Kişisel verilerin kaydedilmesi
(TCK m.135)



Verileri hukuka aykırı olarak verme veya ele geçirme
(TCK m.136)



Rızanız Varsa Suç Oluşmaz.

Kişisel verilerinizin sosyal medyada paylaşılması konusunda, eğer rıza verirsiniz ve bu rızayı anlayarak verirsiniz, ebeveyniniz bakımından suç oluşmaz ve cezai sorumluluk doğmaz.

Verdiğiniz rızanın sonuçlarını anlayabiliyor iseniz, rızanız hukuki olarak geçerlidir. **Bir paylaşım için izin vermek, o paylaşımın sonuçlarını anladığınız anlamına gelir.**

Rıza Vermeden Önce Kendinize Şu Soruları Sorun:

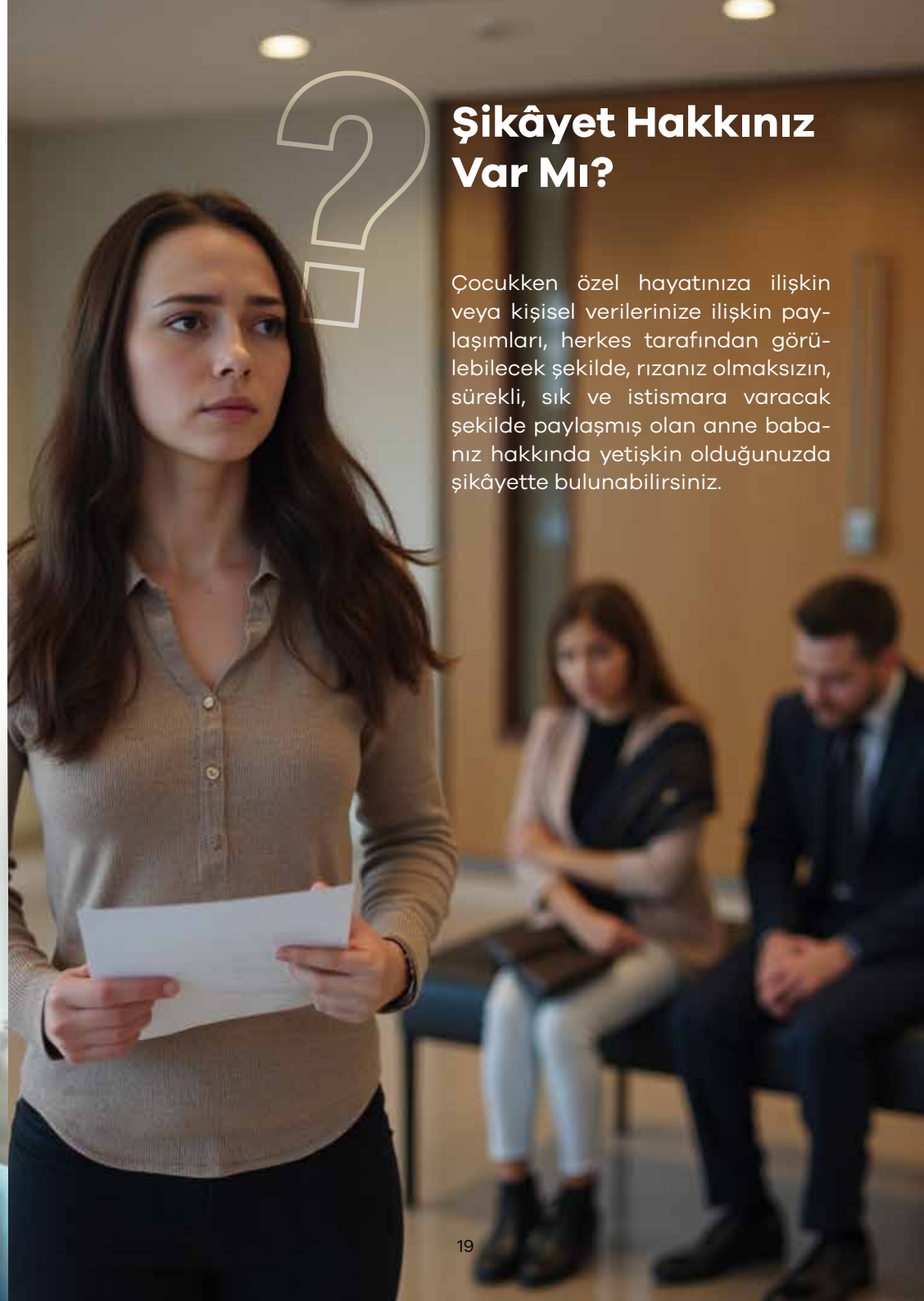
- Bu paylaşımı gerçekten istiyor muyum?
- Kimler görebilecek?
- Gelecekte karşıma çıkar mı?
- Gelecekte beni rahatsız eder mi?
- Bugün komik bulduğum bir şey, ileride beni utandırabilir mi?
- Diğer kişiler tarafından kötüye kullanılabilir mi?

Verdiğiniz bir rızayı her zaman **geri alabilirsiniz**. Eğer bir paylaşım sizi rahatsız ediyorsa, **kararınızı değiştirmek en doğal hakkınızdır**.



Şikâyet Hakkınız Var Mı?

Çocukken özel hayatınıza ilişkin veya kişisel verilerinize ilişkin paylaşımları, herkes tarafından görülebilecek şekilde, rızanız olmaksızın, sürekli, sık ve istismara varacak şekilde paylaşmış olan anne babanız hakkında yetişkin olduğunuzda şikâyetle bulunabilirsiniz.





Dijital Açıdan Gizlilik ve Güvenlik Ayarları



İnternette ve sosyal medyada güvenliğinizi için gizlilik ayarlarınızı düzenlemek çok önemlidir. Kişisel verilerinizin kötü niyetli kişiler tarafından ele geçirilmesini önlemek için dikkat etmeniz gereken bazı noktalar vardır.

Sosyal Medyada Gizlilik için Öneriler:

- **Hesaplarınızı "Gizli" moda alın:** Paylaşımlarınızı sadece güvendiğiniz kişiler görebilmeli.
- **Kişisel bilgilerinizi paylaşmayın:** Adınız, telefon numaranız, adresiniz gibi bilgileri herkese açık hale getirmeyin.
- **Ne paylaştığınıza dikkat edin:** Bir fotoğraf veya video paylaşmadan önce gelecekte nasıl etkiler yaratabileceğini düşünün.
- **Gizlilik ayarlarınızı düzenli olarak kontrol edin:** Platformlar zaman zaman gizlilik politikalarını değiştirebilir.

Güçlü Şifreler ve İki Faktörlü Doğrulama



Hesaplarınızın güvenliği için güçlü şifreler oluşturmanız oldukça önemlidir.

Güvenlik anahtarlarıyla ekstra katman oluşturabilirsiniz.

- Hesaplarınız için kullandığınız parolaların hepsinin aynı olmasına özen göstermelisiniz. Bir hesabınızın şifresi çalındığında, aynı şifreyi kullandığınız diğer hesaplar da riske girebilir ve başkaları tarafından ele geçirilebilir.
- Doğum tarihiniz gibi kişisel veriler veya sözlükte bulunan anlamlı kelimeler içeren parolalar, kolayca tahmin edilebilir. Bu tür şifreler, hesabınızın izinsiz erişime açık hale gelmesine neden olabilir. Şifreleriniz adınızı veya doğum tarihinizi içermemelidir.

Güçlü Şifre Oluşturma İpuçları:

Güçlü bir şifre en az 12 karakter içermelidir:

- Büyük-küçük harf (A-Z, a-z)
- Rakam (0-9)
- Özel karakter (!, @, #, \$, %)

Örnek:

- ✗ **Zayıf Şifre:**
Ali1992
- ✓ **Güçlü Şifre:**
S!berGüvenlik2025\$

İki Faktörlü Doğrulama Kullanımı:

Hesaplarınızın güvenliğini artırmak için iki faktörlü doğrulamayı (2FA) etkinleştirin.



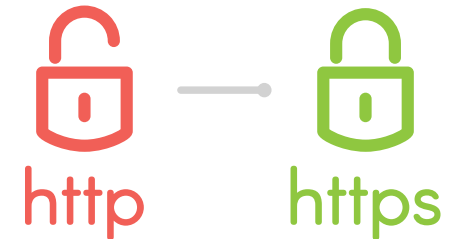
- Google Authenticator, SMS veya e-posta doğrulama yöntemlerinden birini kullanabilirsiniz.
- Şifreniz ele geçirilse bile ikinci adım doğrulama olmadan hesaba giriş yapılamaz.
- Bu kurallara uyarak hesaplarınızı çok daha güvenli hale getirebilirsiniz.



Güvenli İnternette Gezmek İster Misiniz?

İnternette Eğlenirken Güvende Kalın

- Başında "HTTPS" olmayan siteleri kullanmamalısınız.
- İnternet tarayıcısında kilit simgesini kontrol edebilirsiniz. Kilit varsa site güvenlidir. Eğer site adının yanında kilit simgesi yoksa kişisel bilgilerinizi asla paylaşmamalısınız.
- İnternetteki zararlı içeriklerden korunmak için Güvenli İnternet hizmetini kullanabilirsiniz.



Güncellemeler Sizi Güvende Tutar

Eski Sürümlere Elveda. Cihazınızı Hep Güncel Tutmalısınız

- Telefonunuz ya da bilgisayarınız, tıpkı bir süper kahraman gibi, her zaman güçlü ve hızlı olmalıdır. Cihazlarınızın her zaman en iyi şekilde çalışmasını sağlamak için güncellemeleri unutmamalısınız. Gelin, güncellemelerin neden önemli olduğunu keşfedelim.

Güncellemeler Güvenliği Artırır

- Güncellemeler, telefonunuzu ve bilgisayarınızı korur. İnternette dolaşırken kötü niyetli kişiler cihazınızı hedef alabilir. Ancak, güncellemeler cihazınızı koruyarak güvenliğinizi sağlar. Cihazınızdaki güvenlik açıklarını kapatır ve sizi kötü yazılımlardan (virüsler, casus yazılımlar vb.) korur.

Hızlı ve Verimli Çalışır

- Cihazlarınız zamanla yavaşlayabilir. Ancak yeni güncellemeler, cihazdaki yazılımları düzeltir ve hızlanmasına yardımcı olur.

Uygulamalar Daha İyi Çalışır

- Telefon ve bilgisayarınızdaki oyunlar veya uygulamalar güncellendiğinde, daha hızlı çalışır ve hatalar daha az olur.

Eski Yazılımlar Güvenlik Açıklarına Davetiye Çıkarır

- Telefon, tablet ve bilgisayarınızda yazılımları güncelleyerek güvenlik açıklarınızı kapatabilirsiniz.



Wi-Fi Ücretsiz mi? Bedelini Siz Ödemeyin

Wi-Fi, Herkese Açık Olsa da Güvenli Değildir.

Wi-Fi Nedir?

- Wi-Fi, internet bağlantısını kablosuz olarak sağlamak için kullanılan bir teknolojidir. Telefon, tablet ve bilgisayar gibi cihazlar, Wi-Fi sayesinde internete bağlanabilir. Bazı yerlerde, örneğin kafelerde, alışveriş merkezlerinde ve okullarda Wi-Fi herkesin kullanımına açıktır.

Herkese Açık Wi-Fi'nin Zararları

- **Bilgilerinizi Çalabilirler**

Herkese açık Wi-Fi'yi kullandığınızda, internet üzerindeki bilgilerinizi çalmak isteyen kötü niyetli kişiler olabilir. Örneğin, kişisel bilgileriniz, oyun hesaplarınız veya sosyal medya şifreleriniz tehlikeye girebilir.



• Güvensiz Bağlantılar

Herkese açık Wi-Fi, şifrelenmemiş yani korunmasız bir bağlantıdır. Bu da demektir ki, internet bağlantınız "açık" ve herkes görebilir. Tıpkı bir günlüğün sayfalarını açık bırakmak gibi.

• Kötü Yazılımlar Bilgisayarınıza Sızabilir

Bazı insanlar, açık Wi-Fi'yi kullanarak kötü yazılımları (virüsleri) bilgisayarınıza, telefonunuza veya tabletinize gönderebilir. Bu yazılımlar, cihazınızı bozar veya gizli bilgilerinizi çalabilir.

Peki, Ne Yapmalısınız?

• Herkese Açık Wi-Fi Kullanırken Dikkatli Olun

Herkese açık Wi-Fi'yi kullanırken, kişisel bilgilerinizi paylaşmamaya özen göstermelisiniz. Örneğin, şifrelerinizi girmemelisiniz veya banka işlemlerinizi yapmamalısınız.

• Şifreli Wi-Fi Bağlantısı Kullanın

Eğer bir Wi-Fi bağlantısının şifresi yoksa, ona bağlanmamaya çalışın. Şifreli Wi-Fi bağlantıları, bilgilerinizin güvende olmasına yardımcı olur.

• Wi-Fi Bağlantısını Kapatmayı Unutmayın

İnternete bağlandıktan sonra, Wi-Fi bağlantısını kapatmak her zaman iyi bir fikir olabilir. Özellikle seyahat ediyorsanız, gereksiz yere Wi-Fi'ye bağlanmamak güvenliğinizi artırır.

Çerezler ve Dijital İzler

İnternette gezinirken fark etmeden dijital izler bırakabilirsiniz. Çerezler, arama geçmişiniz ve sosyal medya etkileşimleriniz, **hangi içeriklerle ilgilendiğinizi ve hangi siteleri ziyaret ettiğinizi kaydedebilir.** Bu bilgiler bazen size özel öneriler sunmak için kullanılır, ancak bazı durumlarda **gizliliğinizi ihlal edebilir.**

Çerezler Nedir ve Ne İşe Yarar?

- **Çerezler (Cookies)** → Web sitelerinin sizi hatırlamasını sağlar.
- **Tarama Geçmişi** → Ziyaret ettiğiniz siteleri kaydeder.
- **Reklam Takibi** → İlgi alanlarınıza göre size reklam gösterir.
- **Hedefleme ve Profil Çıkarma** → Kişisel verilerinizi analiz eder.

Dijital İzler ve Riskleri

- **Takip Edilme:** Web siteleri, hangi içeriklere tıkladığınızı kaydedebilir.
- **Kişisel Verilerin Kullanılması:** Bazı çerezler, kişisel bilgilerinizi üçüncü taraf şirketlerle paylaşabilir.
- **Anonimliğin Kaybolması:** İnternette yaptığınız her hareket sizi tanımlamak için kullanılabilir.



Çerezleri ve Dijital İzleri Kontrol Altına Alın

- **Gizlilik Ayarlarınızı Güncelleyin:** Çerezleri yönetmek için tarayıcınızın gizlilik ayarlarını düzenleyin.
- **Tarama Geçmişinizi Düzenli Olarak Temizleyin:** Bilgilerinizin kaydedilmesini önleyin.
- **“Özel Mod” Kullanın:** Gizli sekme (incognito) kullanarak iz bırakmadan gezin.
- **Çerezleri Reddetme Seçeneğini Kullanın:** Web sitelerinde “Çerezleri Kabul Etme” seçeneğini değerlendirin.



Uygulamalar ve Kişisel Veriler

Kullandığımız uygulamalar ve internet siteleri, çoğu zaman fark etmeden **kişisel verilerimizi toplar**. Bu veriler, reklam şirketleri tarafından kullanılabilir veya kötü niyetli kişilerin eline geçebilir. **Bu yüzden, uygulamalara hangi izinleri verdiğinize dikkat etmelisiniz.**



Uygulamalar Hangi Verilerinizi Toplayabilir?

- 📍 **Konum Bilgisi** → Nerede olduğunuzu takip edebilir.
- 📷 **Kamera ve Mikrofon** → Sesinizi ve görüntünüzü kaydedebilir.
- 📞 **Rehber ve Mesajlar** → Kişi listenizi ve özel mesajlarınızı görebilir.
- 🕒 **Tarama Geçmişi** → Hangi siteleri ziyaret ettiğinizi öğrenebilir.

Bazı Popüler Uygulamalar Şu İzinleri İsteyebilir:

- 📘 **Facebook & Instagram** → Konum, mikrofon, kamera, rehber
- 🎵 **TikTok** → Kamera, mikrofon, klavye hareketleri, konum
- 💬 **WhatsApp** → Mikrofon, kamera, rehber, mesaj geçmişi
- 📍 **Google Maps** → Konum, cihaz hareketleri, ağ bağlantıları

Uygulama İzinlerini Yönetmek İçin Ne Yapmalısınız?

- **Uygulama yüklerken izinleri inceleyin** → Gereksiz izinler vermeyin.
- **Konum, mikrofon ve kamera izinlerini kapatın** → Sadece ihtiyacınız olduğunda açın.
- **Gizlilik ayarlarınızı düzenli olarak kontrol edin** → Sosyal medya ve uygulamalar zamanla izinlerinizi değiştirebilir.
- **Arka planda çalışan uygulamalara dikkat edin** → Bazı uygulamalar fark etmeden veri toplayabilir.

Tanımadıklarımıza "Hayır" Deme Cesareti

Özellikle şu durumlara dikkat etmelisiniz:

- İnternette tanımadığınız kişilerden gelen mesajlara dikkat etmelisiniz.
- Eğer biri size şüpheli bir **hediye kazandı** veya kişisel bilgilerinizi istemek için mesaj attıysa, mesajı hemen silmelisiniz.
- Her zaman güvendiğiniz bir büyüğüne danışarak daha güvende olabilirsiniz.



Sanal Dünyada Güvenlik Testi

Bu kısa testle dijital gizliliğini ne kadar iyi koruduğunuzu öğrenebilirsiniz.

Her 'EVET' cevabına 10 puan verin. **Toplam puanını hesaplayın ve sonucunu öğrenin!**

Soru	Evet (10 Puan)	Hayır (0 Puan)
Sosyal medya hesaplarınızı özel moda aldınız mı?		
Şifrelerinizi harf, rakam ve özel semboller kullanarak oluşturuyor musunuz?		
Aynı şifreyi farklı hesaplarda kullanmıyor musunuz?		
İki faktörlü kimlik doğrulamayı (2FA) aktif hale getirdiniz mi?		
Tanımadığınız birinden gelen bağlantıya tıklamadan önce düşünür müsünüz?		
Uygulama izinlerini yüklemeyi kontrol ediyor musunuz?		
Halka açık Wi-Fi ağlarında önemli işlemler yapmamaya dikkat ediyor musunuz?		
Çerezleri ve tarama geçmişini düzenli olarak temizliyor musunuz?		
Bilmediğiniz bir uygulamayı yüklemeyi araştırıyor musunuz?		
Paylaşmadan önce bir içeriğin gelecekteki etkilerini düşünüyor musunuz?		

SONUÇLAR:

80-100 Puan → Siber Güvenlik Ustası!

Tebrikler! Dijital dünyada en iyi şekilde korunuyorsunuz. Güvenliğinize dikkat etmeye devam ediniz!

50-70 Puan → Dijital Savunmacı!

Fena değil! Ancak birkaç güvenlik açığınız olabilir. Ayarlarınızı gözden geçirerek kendinizi daha iyi koruyabilirsiniz.

0-40 Puan → Siber Risk Altında!

Dikkat! Dijital dünyada gizliliğiniz risk altında olabilir. Kitapçıkta öğrendiğiniz ipuçlarını uygulayarak güvenliğinizi artırabilirsiniz!

TEŞEKKÜRLER...

Bu rehber kitapçığın sizlere faydalı olmasını, dijital dünyada size destek olmasını ve tehlikeler, riskler konusunda güvenli bir yol haritası çizmeniz için size yardımcı olmasını temenni ediyoruz.

Psikoloji, hukuk ve dijital güvenlik alanlarındaki araştırmalarımızdan siz çocuklar için faydalı olabilecek bilgileri bir araya getirmek bizim için sevgi dolu bir süreç oldu.

Yorum, soru ve önerileriniz olursa, bizimle iletişime geçmenizden mutluluk duyarız: info@dijitalebeveynrehberi.com.

Bu çalışma, Türkiye Bilimsel ve Teknoloji Araştırma Kurumu (TÜBİTAK) tarafından "223K804" numaralı proje ile desteklenmiştir. Projeye verdiği destekten ötürü TÜBİTAK'a teşekkürlerimizi sunarız.

Bu rehber kitapçık, çocukların ebeveynleri tarafından kişisel verilerinin sosyal ağlarda paylaşılması konusunda, **çocukların haklarının ihlal edilmemesine** ve onların dijital dünyanın tehlikelerinden korunmasına **yönelik hedeflerimizin sadece başlangıcıdır**.

Bu kitapçık çevrimiçi olarak dijitalebeveynrehberi.com sitesinde yer almaktadır. Kitapçığın daha fazla çocuk ve ebeveyne ulaşması için sizlerden destek bekliyor, diğer kitapçık ve bilgilerin yer aldığı sitemizi sık sık ziyaret etmenizi temenni ediyoruz.



ÇOCUKLARIN KİŞİSEL VERİLERİ: EBEVEYNLER, PAYLAŞIM ve KORUMA

ÇOCUKLARA YÖNELİK KİTAPÇIK

Bu kitapçık, çocukların kişisel verilerinin korunmasının önemini vurgulamak, ebeveynleri tarafından sosyal ağlarda paylaşıldığında doğabilecek risklere dikkat çekmek, kişisel verilerini ve haklarını nasıl koruyabilecekleri konusunda **çocukları** bilgilendirmek amacıyla hazırlanmıştır.

Bu kitapçık, "223K804" numaralı, "Çocuğun Kişisel Verilerinin Ebeveyni Tarafından Sosyal Ağlarda Paylaşılmasının Psikolojik ve Hukuki Açıdan İncelenmesi" isimli TÜBİTAK projesi kapsamında hazırlanmıştır.