

Yetiřkinlere ve Ebeveynlere Dijital Öneriler

#KiřiselVerilerinveMahremiyetinKorunmasıProgramı

© 2020 - Tüm hakları saklıdır.

Bu doküman (Gençlere Dijital Tavsiyeler) Facebook ve İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü iş birliği ile "**Kişisel Verilerin ve Mahremiyetin Korunması Programı**" kapsamında hazırlanmıştır.

Dokümana çevrim içi ulaşmak için:

<https://itlaw.bilgi.edu.tr/tr/haberler/kisisel-verilerin-ve-mahremiyetin-korunmasi-prog-2-149/>

Tasarım: Pikan Ajans

1. Özel Hayatın Gizliliğinin ve Kişisel Verilerin Korunması

Her bilgi bir veridir. Kişisel veri ise **kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi** ifade eder. Adınız, soyadınız, doğum tarihiniz, fotoğrafınız, parmak iziniz gibi doğrudan sizi gösteren veriler dışında, çeşitli verilerin kümelenmesi sonucunda sizi işaret edebilecek olan veriler de kişisel verinizdir.



Örneğin; internette gezdiğiniz sayfalar veya **Internet Protokol (IP)** adresiniz (internet üzerinde farklı cihazların birbiriyle iletişime geçmesini mümkün kılan sanal adresiniz) ilk bakışta sizinle bağdaştırılamasa da başka verilerle bir araya getirilerek kolayca kim olduğunuza işaret edebilir.



Yaptığınız her hareketle dijital ortamda arkanızda bir iz bırakırsınız. Bu izler zamanla birikir ve hakkınızda sizin bile farkında olmadığınız bilgilere işaret edebilir. Ziyaret ettiğiniz internet siteleri, sosyal medya ve oyun platformları; kullandığınız cihazların tanıtıcı bilgileri (cihaz türü, kimlik bilgisi gibi),

konumunuz, izlediğiniz içerikler, başka hangi siteleri ziyaret ettiğiniz, bir internet sayfası veya uygulama üzerinde ne kadar süre geçirdiğiniz gibi pek çok bilgiyi elde edebilirler. Bunların her biri sizinle ilişkilendirilebildiği ölçüde kişisel veridir.

Hakkınızdaki her bilgi kişisel veridir fakat her bilgi mahrem bilgi değildir. Mahrem bilgi, diğer kişisel verilerinizden farklı olarak herkesin bilmesini istemeyeceğiniz ve özel hayatınıza dair bilgilerdir. Bu tür bilgilerin, gerek kişisel verilerin korunması, gerek mahremiyetin/özel hayatın gizliliğinin korunması hakları kapsamında korunması gerekir.

Unutmayın, kişisel verilerinizin ve mahremiyetinizin/özel hayatınızın gizliliğinin korunmasını istemek temel haklarınızdır.

Yaptığınız her paylaşım sizin dışınızda, başkalarının da kişisel verilerini içerebilir. Bu yüzden paylaşım yaparken dikkatli olmalı ve başkalarının haklarına da saygı göstermelisiniz.



Ebeveynler İçin

Çocuklarınızın fotoğraflarını veya özel bilgilerini paylaşıyorsanız onun kişisel verilerini paylaşıyorsunuz demektir! Çocuğunuzun 18 yaşından küçük olması hiçbir şey değiştirmez! Hatta 18 yaşından küçük olması çevrim içi koruma ihtiyacının daha yüksek olduğunu ve ebeveynlerin daha dikkatli olması gerektiğini anlamına gelir. Çocuğunuzun rızası olmadan bu tür paylaşımları yapmak, onların gizliliğini ve kişisel verilerinin korunmasını ihlal etmektir. Bu yüzden paylaştıklarınıza dikkat edin!



Çocuğunuzun fotoğraf ya da videosunu paylaşmadan önce kendinize şu soruları sorun:

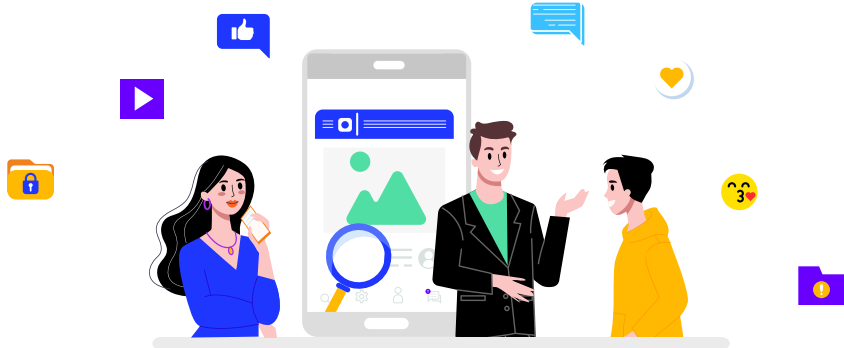
Eğer çocuğunuz belli bir yaş üzerinde ise onun görüşünü aldınız mı?

Bu paylaşım ileride çocuğumun hayatını nasıl etkiler?
Çocuğunuz ileride bu paylaşımından utanabilir mi?

Çocuğunuzun kimliği bu paylaşımında seçilebilir mi?

Bu fotoğraf başkalarının eline geçerse sizin veya çocuğunuz için problem teşkil eder mi?

Çocuğunuzun kişisel verisini sosyal medya platformları ve arkadaş listenizde ekli üçüncü taraf ve kişilerle paylaşmak konusunda ne hissediyorsunuz?



2. Dijital Haklar, Özgürlükler ve Sınırları

Unutmayın, kişisel verilerin ve mahremiyetin/özel hayatın gizliliğinin korunmasını istemek temel bir haktır. Bu hakkınızı hem kendiniz hatırlayın hem de çevrenizdekilere hatırlatın.



Özel hayatın gizliliği ve **kişisel verilerinin korunması** anayasal bir haktır; tıpkı eğitim hakkı, yaşam hakkı, ifade özgürlüğü hakkı gibi. Anayasal hak, bütün haklar üzerinde en çok korunan ve başkaları tarafından ihlal edilmesi durumunda ağır sonuçları olan hak grubudur.

Özel hayatın gizliliğine müdahale eden veya kişisel verileri hukuka aykırı şekilde kullanan kişiler **Türk Ceza Kanunu (TCK)** kapsamında cezalandırılmaktadır. **TCK**'da düzenlenen ilgili suçlar, özel hayatın gizliliğinin ihlali, haberleşmenin gizliliğinin ihlali, kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması, kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve benzeri diğer suçlardır.

Ebeveynler İçin

Örneğin;

Sizin veya başka birinin çocuğunuzun içinde bulunduğu bir fotoğrafı veya bilgiyi paylaşması;

Çocuğunuzun konuşmalarının dinlenmesi ve kaydedilmesi;

Çocuğunuzun kişisel verilerinin sizin ve onun haberi olmadan kaydedilmesi ve kullanılması suçtur!

Ayrıca kişisel veriler **Kişisel Verilerin Korunması Kanunu (KVKK)** kapsamında da korunmaktadır. **KVKK**'ya göre verileri işleyen kişilerin, örneğin sosyal medya platformlarının, gerçekleştirdikleri bu veri işlemeden dolayı sorumlulukları vardır.

KVKK'ya göre dijital alanda sahip olduğunuz haklar aşağıdaki gibidir:

Kişisel verilerin işlenip işlenmediğini öğrenmek,

Kişisel veriler işlenmişse buna ilişkin bilgi talep etmek,

Kişisel verilerin işlenme amaçlarını ve verilerin bu amaçlara uygun kullanılıp kullanılmadığını öğrenmek,

Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilmek, Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini istemek,

Kişisel verilerin silinmesini veya yok edilmesini istemek,

Kişisel verilerin düzeltilmesi, silinmesi veya yok edilmesine ilişkin işlemlerin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini istemek,

İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etmek,

Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etmek.

Kişisel verilerinizin korunması hakkında daha fazla bilgi için <https://kvkk.gov.tr> sitesini ziyaret edebilir, ayrıca KVKK'nın hazırlamış olduğu "**Kişisel Verilerin Korunması Kanunu Hakkında Doğru Bilinen Yanlışlar**" ve "**Örneklerle Kişisel Verilerin Korunması**" belgelerini inceleyebilirsiniz.

Ayrıca, **BTK**'nın bir çalışması olan "**Güvenli Web**"deki [bu sayfayı](#) ziyaret ederek dijital hak ve sorumluluklarınızla ilgili daha detaylı bilgi alabilirsiniz.

Ebeveynler İçin

Kişisel verilerin ve mahremiyetin/özel hayatın gizliliğinin korunmasını istemek temel bir haktır. Bu temel hakkın ne kadar önemli olduğunu çocuğunuzla mutlaka paylaşın.



Çocuğunuzun kendi hakkını bizzat kendisinin savunması konusunda da bilinçlendirin ve eğitin. Bu açıdan Kamu Denetçiliği Kurumu'nun "**çocuk sayfası**" çocuğunuzun bilgilendirilmesi ve eğitiminde kullanabileceğiniz güzel bir örnektir (<https://kdkcocuk.gov.tr/>).

İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü ve Facebook iş birliğinde **Kişisel Verilerin ve Mahremiyetin Korunması Programı** kapsamında hazırladığımız **Çocuklara Dijital Öğütler** kitapçığından da faydalanabilirsiniz.

Her ne kadar verilerin korunması için kanunlar olsa da, tüm sorumluluğu devlete ya da çocuğunuzun okuluna bırakmayın! Çocuklarınızın haklarından haberdar olduğundan emin olun, ve bu hakların ihlal edilmemesi için çocuğunuzla birlikte hareket edin!

3. Çevrim içi Tehlike ve Riskler

Sosyal medya platformları, çevrim içi oyunlar gibi ortamlarda aşağıda sıraladığımız gibi çeşitli rahatsız edici veya tehlikeli durumlarla karşılaşabilirsiniz.

Hakaret:

Onur kırıcı, küçültücü söz ve davranışlardır.

Siber zorbalık:

Siber zorbalık, çevrim içi ortamlar aracılığıyla gerçekleştirilen ve hedef seçilen kişiye rahatsızlık vermek, kızdırmak, utandırmak, üzme için yapılan her türlü davranıştır. Aşağılama, iftira, her türlü asılsız beyan, taciz, tehdit ve dışlama gibi davranışlar siber zorbalığa örnektir.



Doxing:

Hedef seçilen kişi hakkında internet veya sosyal medya hesapları üzerinden ulaşılabilen tüm bilgilerin derlenerek internette herkesin erişebileceği şekilde yayınlanması, bu yolla hedef seçilen kişinin özel hayatının gizliliğinin ihlal edilmesi, utandırılması ve zor durumda bırakılmasıdır.

Sosyal medyada, oyun platformlarında veya internette gezinirken istenmeyen reklamların gösterilmesi, reklam amaçlı istenmeyen e-posta ve mesajlar (spam),

Müstehcen veya uygunsuz içeriklerle karşılaşmak, uygunsuz içerikli mesajlar almak (örneğin: pornografi, cinsel içerikli görüntü ve mesajlar).

Kişisel veri istismarı:

Kişisel verilerin, özellikle de şifrelerin, başkalarının eline geçmesi, bu istismara uğrayan kişilerin korkutma ve tehditle istismar edilmesidir. Dolandırılma veya kandırılma: Oyun içi satın alma işlemlerinde dolandırıcılıkla karşılaşabilirsiniz veya kötü niyetli kişiler sizi e-posta veya özel mesajlarla kendi amaçları doğrultusunda kandırmaya ve yönlendirmeye çalışabilir (scam).

Dolandırılma veya kandırılma:

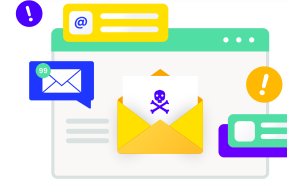
Oyun içi satın alma işlemlerinde dolandırıcılıkla karşılaşabilirsiniz veya kötü niyetli kişiler sizi e-posta veya özel mesajlarla kendi amaçları doğrultusunda kandırmaya ve yönlendirmeye çalışabilir (scam).

Catfishing:

Sosyal medya veya çevrim içi iletişim araçları kullanılarak sahte bir kimlik yaratılması, bu sahte kimlik kullanılarak hedef seçilen kişinin, maddi kazanç elde etmek, romantik ilişki kurmak gibi çeşitli amaçlarla kandırılması ve/veya dolandırılmasıdır.

Sosyal medya hesaplarının ele geçirilmesi/hacklenmesi,

Başka biriymiş gibi davranan sahte hesaplar.



Grooming:

Cinsel veya duygusal istismar amacıyla çocuklarla iletişim kurulması, arkadaşlık edilmesi ve çocuğun bu iletişim sonunda bazı davranışlara zorlanmasıdır.

Sextortion:

Kişilerin müstehcen görüntülerini ve bilgilerini çeşitli yollarla ele geçiren kimselerin, bunları kullanarak mağduru kendi istekleri doğrultusunda hareket etmeye zorlaması ve şantaj yapmasıdır.

Yalan Haberler:

İnternette karşılaşılan her bilgi ve haberin doğru değildir. Günümüzde kötü niyetli pek çok kişi ve grup, hem bireyleri hem de toplumları yönlendirmek amacıyla yalan haberler üretilip yaymaktadır. Karşılaşılan haber ve içeriklerin kaynağı kontrol edilmeli ve mümkünse okunulan haberin doğruluğu birden fazla kaynaktan teyit edilmelidir.

İnternet bağımlılığı/Aşırı internet kullanımı:

Kontrol edilemeyen ve bağımlılık seviyesine ulaşan internet kullanımı uykuyu, genel olarak sağlığı, sosyal yaşantıyı, eğitim veya iş hayatını olumsuz etkileyebilir.

Ebeveynler İin

ocuėunuz veya etrafınızdaki ocuklar da yukarıdaki olumsuz durumlar ile karřılařıyor olabilirler. ocuėunuzu bu konuda nasıl eėitebilirsiniz?

Ona haklarını anlayabileceėi bir řekilde anlatın. Bu kitapıkta bahsedilen haklarının altını izerek ona yardım edecek insanların her zaman olacaėını hatırlatın.

Bir problemle karřılařtıėında sizinle ekinmeden konuřabileceėini sylediėinizden emin olun.

Dijital ortamda yaptığı hiçbir řeyden utanmaması gerektiėi dřuncesini ařılayın. Kt bir duruma dřtėnde bunu sizinle paylařırsa sorun ne olursa olsun zlebiyeceėini hatırlatın.

Mmknse oyun ve sosyal platformlarındaki sohbet etme fonksiyonunu kapatmasını tembihleyin. Gerek hayatta tanımadığı kimse ile evrim ii ortamda da sohbet etmek zorunda olmadıėını sık sık hatırlatın! ocuklarınıza grooming gibi karřılařabilecekleri risklerden bahsedin, farkındalıklarını arttırın.

Gerek hayatta tanımadığı birinin evrim ii ortamda da arkadařlık teklifini kabul etmemesi gerektiėini ğretin. Dijital ortam insanlarla tanışmak iin eėlenceli bir yer olsa da, bu platformları zaten tanıdığı insanlarla etkileřmek iin kullanmasını destekleyin.

Diėer aileler ve okul ile iletiřimde olun! Bařka ocukların internette yapabildiėi řeylerden kendi ocuėunuzu mahrum bırakmak onu sınırlendirebilir, kırabilir. Diėer aileler ve okulu ile ortak bir řekilde hareket ederseniz bu durumu engelleyebilirsiniz.

Dijital dnya ocukların eėitimi, sosyalleřmesi ve eėlenmesi iin olduka faydalı bir aratır. Her ne kadar evrim ii ortamda tehlike ve riskler olsa da, ocuklarınızı dijital platformlardan tamamiyle koparmak yerine onlara gvenli bir ortam yaratarak; dijital platformlardan yaratıcılıklarını geliřtirmek, diledikleri eėitimi alarak kiřisel geliřimlerini destekleyecek řekilde yararlanmalarını saėlayabilirsiniz. ocukların kiřisel verilerinin etkin řekilde korunması adına **KVKK** tarafından hazırlanan ve pratik nerilerin yer aldıėı kitapıkları okuyabilirsiniz: <https://www.kvkk.gov.tr/Icerik/6737/Cocukların-Kişisel-Verilerinin-Korunması-Bakimından-Dikkat-Edilmesi-Gerekenler>



4. Çevrim içi Ortamda İfade Özgürlüğü ve Hoşgörü

Türkiye Cumhuriyeti Anayasası'na göre; herkes, düşünce ve ifade özgürlüğüne ve bunları açıklama ve yayma hakkına sahiptir. Bu hakkın korunması demokratik toplum için gereklidir. Yaş sınırı olmaksızın ifade özgürlüğü toplumun her bireyi için tanınmış temel hak ve özgürlüktür.



İnternette herkesin düşüncelerini dilediği gibi ifade etme hakkı vardır fakat bu hakkın bir sınırı da bulunmaktadır.

Siber zorbalık, bu sınırın aşıldığı bir örnektir ve çevrim içi ortamda karşılaşılan en ciddi problemlerden biri haline gelmiştir.

Siber zorbalık, hedef seçilen kişiye rahatsızlık vermek için yapılan her türlü davranışı kapsar. Aşağılama, iftira, her türlü asılsız iftira, taciz, tehdit ve dışlama gibi davranışlar siber zorbalığa örnek oluşturur.

Ebeveynler İçin

Hoşgörüğü ilk önce evde, kendi aranızdaki konuşmalarda altını çizerek uygularsanız, çocuğunuzun dijital ortamlarda bu tür hareketlerden kaçınmasını sağlayabilirsiniz. Onlara kendi hareketlerinizle örnek olabileceğinizi unutmayın!



5. Farkındalık ve Kontrol Platform İçi ve Platform Dışı Yöntemler

Ebeveynler İçin

Sosyal medya ve çevrim içi oyun platformlarında çocuğunuzun en etkin şekilde korumak için ne yapmalısınız?

Platform İçi Araçlarla Gizlilik ve Kişisel Veri Koruması



Sosyal medyada size sunulan [ayarları](#) ve kontrol seçeneklerini en etkili şekilde kullanabilirsiniz. Çocuğunuzun sosyal medya platformlarının gizli olduğundan emin olun.

Oyunların ve sosyal medya platformlarının koyduğu yaş sınırlamasını dikkate alın.

Aile içinde bu sınırlamalara saygı gösterilmesi gerektiği üzerine bir anlaşmaya varın. Yaş sınırı itibarıyla çocuğunuzun kullanmaması gereken sosyal medya platformları mevcut. Ebeveyn olarak sizin göreviniz çocuğunuzun bu platformları kullanmadığından ve interneti güvenli bir şekilde kullandığından emin olmak. Çocuğunuza **Messenger Kids** gibi çocuklara özel olarak geliştirilmiş sosyal medya platformlarını kullanabileceğini söyleyebilirsiniz.

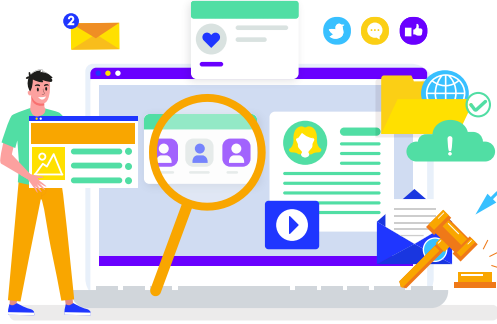
İster kendinizin isterse çocuğunuzun hesabı olsun, deneyiminizden en iyi şekilde yararlanmak ve çocuğunuzun deneyimini yönlendirmeye yardımcı olmak için Facebook'un hazırlamış olduğu [Ebeveyn Portalı](#)na bakabilirsiniz.

Çocuğunuza, çevrim içi platformlarda zorbalıkla karşılaşırsa ona zorbalık yapan kişiye karşılık vermeye çalışmamasını ama kendisine zorbalık yapan kişinin onu bastırmasına izin vermemesi gerektiğini öğretin.

Çocuklarınıza güven vermeyi, karşılaştıkları olumsuz bir durum olur ise size anlatabileceklerini söylemeyi ve hukuki yollara başvurabileceğinizi unutmayın.

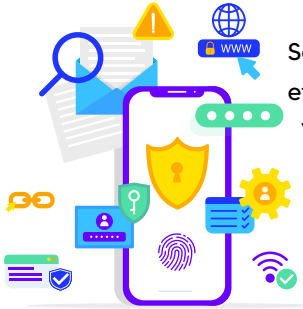
Birçok platform kullanıcılarına diğer kullanıcıları engelleme ve şikayet gibi seçenekler sunmaktadır. Kişiyi arkadaşlarınız arasından çıkarabilir, şikayet edebilir ve engelleyebilirsiniz. Kişiyi şikayet edebileceğiniz gibi, sizinle veya başkalarıyla paylaşılan kötü amaçlı paylaşımları da şikayet etmeniz mümkündür.

Olumsuz bir durumla karşılaşırsanız, bu durumu mutlaka belgeleyin ve kaydedin. Size rahatsızlık veren bir paylaşım ile karşılaşırsanız, gerektiğinde veya talep edildiğinde yetkililerle paylaşabilmek amacıyla bu paylaşımın çıktısını veya ekran görüntüsünü almalı ve saklamalısınız.



Daha fazla bilgi, araç ve kaynak için [İnternet Yardım Merkezi](#)'ni ziyaret edebilirsiniz.

Reklamlardan rahatsız oluyorsanız tercihlerinizi kendiniz [yönetebilirsiniz](#)



Sosyal ağ platformlarında alabileceğiniz önlemler ve şikayet etme yöntemleri hakkında daha detaylı bilgi için İnternet Yardım'ın [Sosyal Ağ Platformları](#) sayfasını ziyaret edebilirsiniz.

Güvenlik Merkezi'nde (<https://www.facebook.com/safety>) çevrim içi güvenlik tavsiyelerini bulabilirsiniz. Bu merkez aynı zamanda çeşitli güvenlik kontrolleri, zorbalığı önlemek için yapılabilecekler gibi konular için de faydalıdır.

Instagram'da çevrim içi güvenlik ve gizliliğe dair ipuçları için [Instagram Yardım Merkezi](#)'ni ziyaret edebilirsiniz. Ayrıca [Instagram Wellbeing Çalışmaları](#)'na bakabilirsiniz.

[WhatsApp Gizlilik](#) bağlantısı üzerinden, çok sık kullanılan bir mesajlaşma uygulaması olan WhatsApp'ta güvenlik ve gizliliğinizi nasıl sağlayacağınızla ilgili bilgilere ulaşabilirsiniz.

Newsroom Posts: Facebook tarafından güncel olarak paylaşılan gelişmeleri [buradan](#) takip edebilirsiniz.

Platform dışı yöntemler:

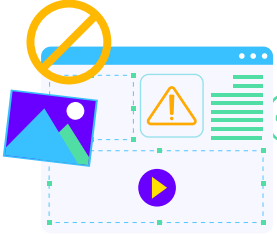
Siber tehditler, dolandırıcılık internet siteleri ve spamler ile ilgili olarak Ulusal Siber Olaylara Müdahale Merkezi ([USOM](#)) siber ihbar sayfasından yardım alabilirsiniz.



Siber zorbalığa son vermek için neler yapabileceğinizi BTK'nın bir çalışması olan **"Güvenli Web"**'in siber zorbalığa ilişkin [bu sitesinden](#) ve Facebook'un zorbalıkla mücadele hakkında hazırlamış olduğu [bu sayfadan](#) öğrenebilirsiniz.

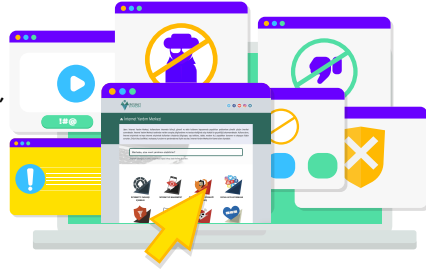
Kişisel verilerin korunmasına dair haklar ihlal edilirse, yukarıda açıkladığımız hakları, veri işleyen platforma başvurarak kullanabilirsiniz. Veri işleyen bu hakları kullanmanıza izin vermezse, süresi içinde **Kişisel Verileri Koruma Kurumu**'na şikayette bulunabilirsiniz.

Kişilik haklarınız ihlal edildiğinde, **Asliye Hukuk Mahkemelerine** başvurarak ihlalin sona erdirilmesini, ayrıca maddi veya manevi bir zarara uğradıysanız tazminat talep edebilirsiniz.



5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'a göre, çocuğunuzun hakkı internet üzerinden bir yayınlı ihlal edilirse içeriğin kaldırılması ve içeriğe erişimin engellenmesi mümkündür. Duruma göre içerik sağlayıcısına, yer sağlayıcısına, sulh ceza hakimine ve Bilgi Teknolojileri ve İletişim Kurumu'na (BTK) başvurulabilir.

Çevrim içi şikayet mekanizmaları: Eğer internet aracılığı ile İntihara Yönlendirme, Çocukların Cinsel İstismarı, Uyuşturucu veya Uyarıcı Madde Kullanılmasını Kolaylaştırma, Sağlık için Tehlikeli Madde Temini, Müstehcenlik, ve İmkân Sağlama, Atatürk Aleyhine İşlenen Suçlar, Yasadışı Bahis gibi suçlardan birinin işlendiğini düşünüyorsanız, [İnternet Yardım](#) sitesine başvurarak platform özelinde ne yapmanız gerektiğine dair bilgi alabilirsiniz. Ayrıca BTK'nın e-devlette bulunan [internet ihbar portalı](#)ndan ve [İnternet Bilgi İhbar Merkezi](#) üzerinden şikayette bulunabilirsiniz.



Cumhuriyet Savcılığı, kolluk kuvvetleri: Yukarıda saydığımız yöntemler sorunu çözmek için yetersiz kalırsa, en yakın Cumhuriyet Savcılığı'na başvurabilirsiniz. Emniyet güçlerine [ihbarda](#) bulunmak için: **155 Polis İmdat** hattı - **155@iem.gov.tr**

Kolluk kuvvetlerine ve savcılığa yapacağınız başvurularda kullanmak üzere siber zorbalık teşkil eden mesajlaşmaları ve ekran görüntülerini kaydedip saklamalısınız.

6. Güvenlik



Özel hayatın gizliliğinin ve kişisel verilerinizin korunmasının ne kadar önemli olduğunu hiç unutmayın!



Güçlü bir şifre seçin (büyük harf, küçük harf, rakam ve "?", "@", "!", "#", "%", "+", "-", "*", "%" gibi özel karakterler kullanabilirsiniz). Uzun ve tahmin edilmesi zor şifreler daha güvenlidir. Aklınızda tutabileceğiniz uzun bir cümleyi şifre olarak belirleyebilirsiniz.



Şifrelerinizi en az 2-3 ayda bir düzenli olarak değiştirin ve kimseyle paylaşmayın.



Ek bir hesap güvenliği önlemi olarak "iki faktörlü kimlik doğrulamasının" açıldığından emin olun.



Aynı zamanda sosyal medya platformlarının ve internet tarayıcılarının sunduğu "yaş sınırlaması" ve Ebeveyn Kontrol Panellerinden yardım olarak da kontrol ve güven sağlayabilirsiniz. Bu ayarları tarayıcının "Ayarlar" sekmesinden belirleyebilir, veya internet sitesine giderek yardım alabilirsiniz. Yaş sınırlamaları bir öneri olarak değil, bir kısıtlama olarak konulmuştur, bu kurallara saygı duyun ve uygulayın.



Başkalarıyla paylaştığınız bir bilgisayarı veya telefonu kullandıktan sonra sosyal medya hesaplarından aynı zamanda e-posta ve üyelik gerektiren bütün platformlar çıkış yapın.



Genel kullanıma açık bir bilgisayardan giriş yaparken "Beni Hatırla" kutusunu işaretlemeyin!





İnternette karşılaşılan reklamları sınırlamak ve daha güvenli bir internet deneyimi yaratmak için reklam engelleme yazılımlarını (Adblocker) kullanabilirsiniz.



Üçüncü parti uygulamalarına izin verirken dikkatli olmalısınız. Uygulamalara verdiğiniz izinleri mutlaka düzenli olarak kontrol edin.



Cihazlarınıza virüs ve casus yazılımları engelleyecek uygulamalar yükleyebilirsiniz, güvenlik duvarını etkinleştirebilirsiniz.

Ebeveynler için

Çocuğunuzun özel hayatının gizliliği ve kişisel verilerinin korunması sizin de elinizde!



Çocuğunuzun güvenliği için yapacağınız hiçbir şeyi ondan gizleyerek yapmayın, her zaman onu haberdar ederek aldığınız önlemlerin nedenini anlatın. Beraber daha güvenli bir dijital hayat yaratabilirsiniz.



Çocuğunuzun kullandığı şifrelerini kendi güvenliği için önemli olduğunu ve bu nedenle çok sevdiği arkadaşları da olsa kimseyle paylaşmaması gerektiğini vurgulayın.



Çocuğunuzun da reklam gösterimi gibi amaçlarla profillenmesini önlemek için, özel olarak çocukların kullanımına özgülenmiş sosyal medya platformlarını tercih edin. Örneğin; **Messenger Kids**.
<https://messengerkids.com/>



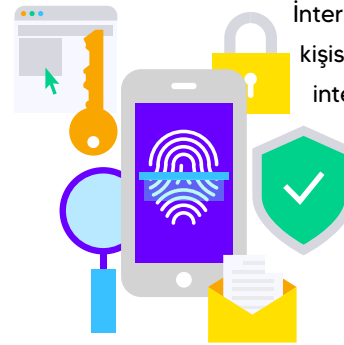
Çocuğunuzun kullandığı cihazlarda, internet tarayıcısına uzantı olarak ekleyebileceğiniz veya doğrudan varsayılan internet tarayıcısı olarak ayarlayarak kontrolü sağlayacağınız tarayıcı ve uzantı listesine <https://globalprivacycontrol.org/> bağlantısından erişebilirsiniz. Listede yer alan "privacy badger" bu amaçla kullanabileceğiniz bir uzantı niteliğinde iken, "duck duck go" kullanıcıların IP adreslerini ve kişisel bilgilerini kaydetmeyen bir tarayıcıdır.



Gerek olmadıkça mikrofon ve kamera kullanımının kapalı olduğundan ve çocuklarınızın herhangi bir platformdaki hesabını başkası tarafından görülmeyecek bir şekilde, onların haberi dahilinde kilitlediğinizden emin olun.

Farkındalığınızı nasıl artırabilirsiniz?

BİLGİ Bilişim ve Teknoloji Hukuku Enstitüsü ve **Facebook** iş birliğinde hazırlamış olduğumuz kaynaklara <https://itlaw.bilgi.edu.tr/tr/haberler/kisisel-verilerin-ve-mahremiyetin-korunmasi-prog-2-149/> ve <https://istasyon.fb.com/tr/programlar/> adreslerinden erişebilirsiniz. Dijital oyunlarla ilgili detaylı bilgiye **Dijital Oyunlar Bilgi Platformu**'nun internet sitesinden ya da **İnternet Yardım Merkezi**'nin **Dijital Oyunlar** sayfasından ulaşabilirsiniz.



İnternet ve mahremiyet hakkında bilgi edinmek, kişisel verileriniz rızanız dışında yayımlandığında veya internet ortamında özel hayatınızın gizliliği ihlal edildiğinde adım adım yapabileceklerinizi öğrenmek için **İnternet Yardım**'ın **İnternet ve Mahremiyet** sayfasını ziyaret edebilirsiniz.

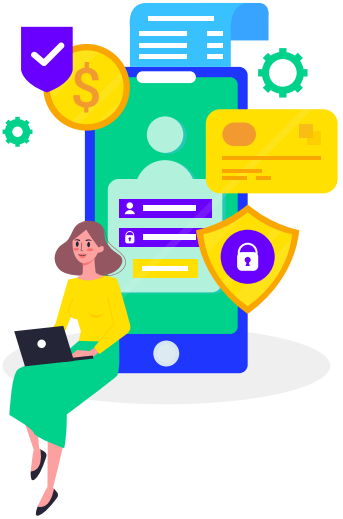
Kişisel verilerin korunması hakkında bilgi almak için **KVKK**'nın hazırladığı bilgilendirici **videoları** da izleyebilir ve **Kişisel Verilerin Korunması Hakkında Sıkça Sorulan Sorular** ve **100 Soruda Kişisel Verilerin Korunması Kanunu** kaynaklarını inceleyebilirsiniz.

Siber zorbalıkla ilgili daha detaylı bilgi edinmek ve mücadele etmek için yapabileceklerinizi adım adım öğrenmek amacıyla, **İnternet Yardım**'ın **Siber Zorbalık** sayfasını ziyaret edebilir, ayrıca **UNICEF Türkiye**'nin hazırladığı **"Siber zorbalık: Nedir ve nasıl önlenir"** başlıklı sayfayı inceleyebilirsiniz.

Siber zorbalık dijital şiddetin bir türüdür. Dijital şiddet ile ilgili daha fazla bilgi edinmek için **BTK**'nın bir çalışması olan **"Güvenli Web"**'deki **"Teknolojiyle birlikte gelen dijital şiddet kavramı"** başlıklı yazısını inceleyebilirsiniz.

Doxing hakkında daha fazla bilgiye, yine **BTK**'nın bir çalışması olan **"Güvenli Web"**'de konuya dair **bu sayfa**dan ulaşabilirsiniz.

İnternette bilgi güvenliği ve alışveriş hakkında bilgi edinmek için yine İnternet Yardım'ın hazırlamış olduğu **İnternet ve Bilgi Güvenliği** sayfasını ziyaret edebilir, ayrıca **BTK**'nın bir çalışması olan **"Güvenli Web"**'deki **"İnternette Güvenli Alışverişin El Rehberi"**ni inceleyebilirsiniz.



Sosyal medya <https://www.siberay.com/sosyal-medya-bagimlilik>, ekran <https://www.siberay.com/ekran-bagimlilik> ve teknoloji bağımlılığı <https://www.siberay.com/teknoloji-bagimlilik> ile ilgili bilgi almak için **Siberay Projesi**'nin <https://www.siberay.com/> sayfasını ziyaret edebilirsiniz.

İnternette dolandırıcılık hakkında bilgi edinmek için ise **BTK**'nın bir çalışması olan **"Güvenli Web"**'deki **"İnternet dolandırıcılarına geçit vermeyin!"** başlıklı haberine göz atabilirsiniz.

İnternette çeşitli yasadışı içeriklerin nasıl şikayet edilebileceğine ilişkin bilgi için **İnternet Yardım**'ın **İnternette Yasadışı İçerikler** sayfasını inceleyebilirsiniz.



BİLGİ Information
Technology Law
Institute

FACEBOOK



İstanbul
Bilgi Üniversitesi