

Gençlere Dijital Tavsiyeler

#KişiselVerilerinveMahremiyetinKorunmasıProgramı

© 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/en/news/genclere-dijital-tavsiyeler-kisisel-verilerin-ve-m-147/>

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.



2. Dijital Haklarınız nelerdir?

Özel hayatınızın gizliliğinin ve **kişisel verilerinizin korunmasını** istemek 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 hayatınızın gizliliğine müdahale eden veya kişisel verilerinizi hukuka aykırı şekilde kullanan kişiler **Türk Ceza Kanunu (TCK)** kapsamında cezalandırılabilir.

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 suçlardır.



Örneğin;

Arkadaşlarınızla olan yazışmalarınızı arkadaşınızın rızası olmadan başkaları ile paylaşmak;

Arkadaşınızın haberi olmadan onun konuşmasını dinlemek ve bir cihaz aracılığıyla kayda almak;

Arkadaşlarınızın kişisel verilerini onlardan habersiz kaydetmek;

Bir başkasının telefonunda bulunan fotoğraflarını onun rızası olmadan almak

ve başkalarıyla paylaşmak suçtur!

Yukarıdaki suçları işleyen kişinin 18 yaşından küçük olması, ceza almayacağı anlamına gelmez. 18 yaşından küçüklere de hapis cezası ve güvenlik tedbiri gibi cezalar uygulanabilir.

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



KVKK'nın haklarınızın açıklandığı başlıklarına göz atarak haklarınızın neler olduğunu öğrenebilirsiniz ve bu haklarınızı sonuna kadar kullanabilirsiniz.

KVKK'ya göre haklarınız aşağıdaki gibidir:

- Kişisel verilerinizin işlenip işlenmediğini öğrenmek,
- Kişisel verileriniz işlenmişse buna ilişkin bilgi talep etmek,
- Kişisel verilerinizin işlenme amaçlarını ve verilerinizin bu amaçlara uygun kullanılıp kullanılmadığını öğrenmek,
- Yurt içinde veya yurt dışında kişisel verilerinizin aktarıldığı başkaca 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.

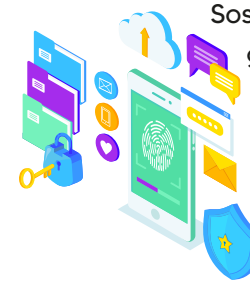
Ayrıca, BTK'nın bir çalışması olan "Güvenli Web"deki [bu sayfayı](#) ziyaret ederek dijital hak ve sorumluluklarınızla ilgili daha detaylı bilgi alabilirsiniz.



3. Çevrim içi Tehlikeler ve Güvenlik Riskleri Nelerdir?

Sosyal medya platformları, çevrim içi oyunlar gibi ortamlarda 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, üzmek 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:** İnternette karşılaştığınız bazı kişiler, çeşitli yararlar sağlamak için sizi dolandırmak ve kandırmak isteyebilir. Örneğin 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).

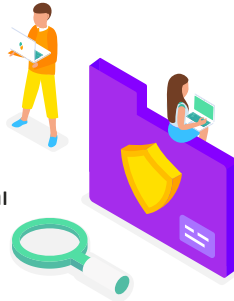
Sosyal medya hesaplarının ele geçirilmesi/hacklenmesi,

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.

- **Cinsel içerikli şantaj (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 karşılaştığınız her bilgi ve haberin doğru olmayabileceğini unutmayın. Günümüzde kötü niyetli pek çok kişi ve grup, hem bireyleri hem de toplumları yönlendirmek amacıyla yalan haberler üretip yaymaktadır. Karşılaştığınız haber ve içeriklerin kaynağını kontrol etmeli ve mümkünse okuduğunuz haberin doğruluğunu birden fazla kaynaktan teyit etmelisiniz.

- **İnternet bağımlılığı:** Kontrol edilemeyen ve bağımlılık seviyesine ulaşan internet kullanımı uykuyu, sosyal yaşantıyı, eğitim veya iş hayatını olumsuz etkileyebilir.

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.

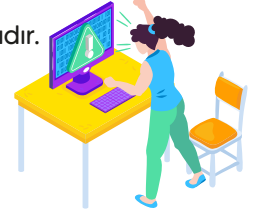
! İnternette herkesin düşüncelerini dilediği gibi ifade etme hakkı vardır, fakat bu hakkın bir sınırı da bulunmaktadır.



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.

Siber zorbalığın da bir şiddet türü olduğu unutulmamalıdır. Yüz yüze ortamlarda gerçekleşmiyor olması, yaşanan olayın şiddet olduğunu ya da şiddetin derecesini azaltmaz.



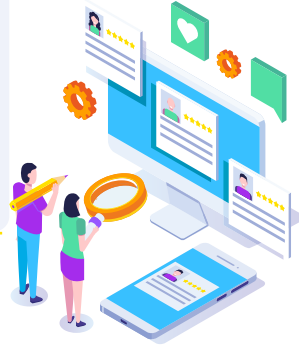
5. Farkındalık ve Kontrol

Platform İçi ve Platform Dışı Yöntemler

Sosyal medya ve çevrim içi oyun platformlarında tanımadığınız bir kişi sizi rahatsız ederse ne yapmalısınız?

Platform İçi Araçlarla Gizlilik ve Kişisel Veri Koruması

- ✓ Sosyal medyada size sunulan **ayarları** ve kontrol seçeneklerini en etkili şekilde kullanabilirsiniz.
- ✓ 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.
- ! Çevrim içi platformlarda zorbalık, taciz ve saldırıyla karşılaşsanız karşılık vermeyin.



- ✓ Durumu mutlaka belgeleyin ve kaydedin. Size rahatsızlık veren bir paylaşım ile karşılaşsanız, 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.



- f **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.



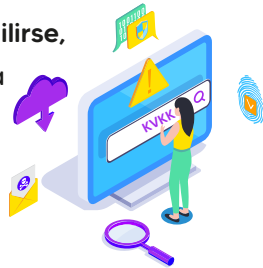
Platform Dışı Yöntemler:

Siber tehditler, dolandırıcılık internet siteleri ve spamler ile ilgili olarak **USOM (Ulusal Siber Olaylara Müdahale Merkezi)** siber ihbar hattından 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 verilerinizin korunmasına dair haklarınız ihlal edilirse, yukarıda açıkladığımız haklarınızı, veri işleyen platforma başvurarak kullanabilirsiniz. Veri işleyen bu haklarınızı 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 uğradiysanız tazminat talep edebilirsiniz.

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'a göre, hakkınız internet üzerinden bir yayınla 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) başvurabilirsiniz. Eğer 18 yaşından küçükseniz ebeveynlerinize haber vermeyi ve hukuki yollara başvurabileceğinizi unutmayın.

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, Fuhuş, Kumar Oynanması için Yer 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 doğrulamasını açın.



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 karşılaştığınız reklamları sınırlamak ve daha güvenli bir internet deneyimi 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.

Farkındalığınızı artırmak ister misiniz?



Facebook Gençlik Portalı'nı ziyaret ederek internette güvenliğinizi nasıl sağlayacağınız hakkında pek çok yararlı bilgi edinebilirsiniz.



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.



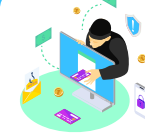
Kişisel verilerin korunması hakkında bilgi almak için **KVKK**'nın hazırladığı bilgilendirici **videoları** da izleyebilir ve **Kişisel Verilerin Korunması Hakkında Sıkça Sorulan Sorular** ve **100 Soruda Kişisel Verilerin Korunması Kanunu** kaynaklarını inceleyebilirsiniz.



Siber zorbalıkla mücadele etmek için neler yapabileceğinizi öğrenmek isterseniz **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.



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.



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.

BİLGİ Information
Technology Law
Institute

FACEBOOK



İstanbul
Bilgi Üniversitesi