



# İNTERNETİN GÜVENLİ KULLANIMI ve SİBER ZORBALIK



**YEŞİLAY**

TÜRKİYE BAĞIMLILIKLA  
MÜCADELE  
EĞİTİM PROGRAMI

**YETİŞKİN**

# Sunum İeriđi

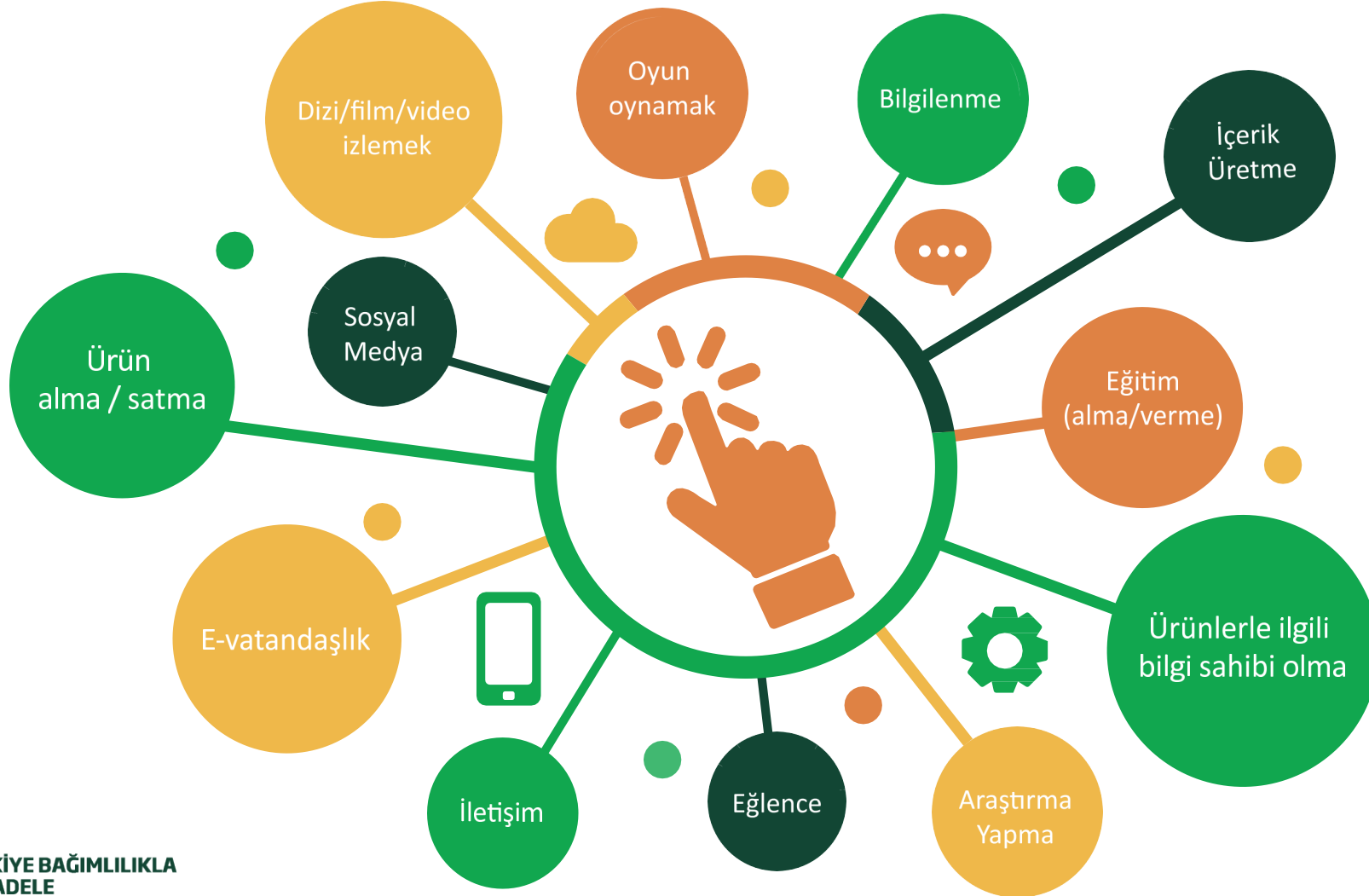
- İnternet ile Neler Yapabiliriz?
- İnternetin Gvenli Kullanımı
- Dijital Dnyanın Riskleri
- İyi Bir Dijital Vatandař Olmak
- Dijital Okuryazarlık
- İnterneti Gvenli Kullanım İin İpuları
- Siber Zorbalık
- Hukuki Boyut



# İnternet ile Neler Yapabiliriz?



# İnternet ile Neler Yapabiliriz?



# İnternetin Güvenli Kullanımı

- İnternet tabanlı uygulamaları kullanan bireylere ait verilerin kötü niyetli kişiler tarafından ele geçirilememesi, gizlilik ihlali olmaması, korunması ve ayrıca bu verilerin kaybolması ya da hasar görmesi durumunda kurtarılabilmesi için güvende tutulmasını kapsar.
- Dijital güvenlik, teknoloji, kazanç ve kişisel kimliği güvence altına alan ve herkesi kapsayan bir kavramdır.



# İnternette Güvenlik İhlalleri



## DİJİTAL AYAK İZİ

Bir televizyon programı, sosyal medyadaki uygunsuz paylaşımları nedeniyle yarışmacısını diskalifiye etti.



## SİBER GÜVENLİK

Bir grup dolandırıcı internet üzerinden sahte alışveriş siteleri kurup, ucuza ürün satma vaadi ile kullanıcıların kredi kartı bilgilerini ele geçirdi. Ortalama yöntemiyle kullanıcıları 350 bin lira dolandırdıkları ortaya çıktı.



## SİBER ZORBALIK

UNICEF'in 30 ülkeyi kapsayan çalışmasının raporuna göre(2019), her üç gençten biri çevrim içi zorbalığa maruz kalıyor, her beş çocuktan biri de siber zorbalık ve şiddet gibi nedenlerle okuluna devam edemiyor.

# Dijital Dünyanın Riskleri

**Davranış Riskleri:** Zorbalık, kasten ya da farkında olmadan insanların yanlış bilgilendirilmesi, yasa dışı indirme, kumar oynama, korsanlık vb.



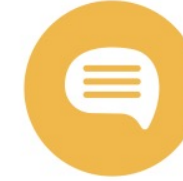
**İletişim Riskleri:** Tacize uğrama, başkaları tarafından rahatsız edilme, siber takip



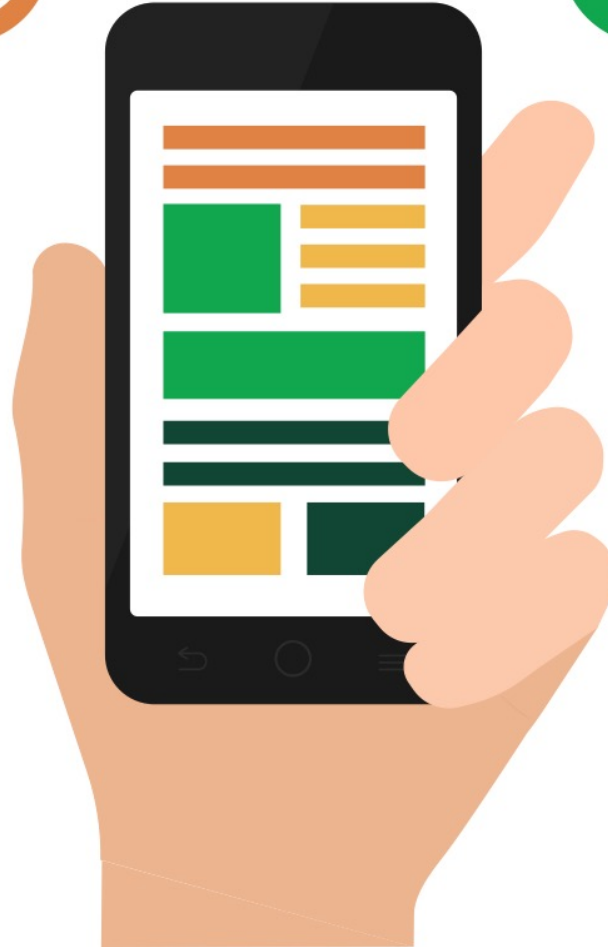
**Ticari Riskler:** Aşırı veya gizli pazarlama, dolandırıcılık vb.



**İçerik Riskleri:** Şiddet, pornografik içerik, cinsiyetçi, ırkçı veya nefret söylemi içeren materyaller de dahil olmak üzere potansiyel olarak saldırgan veya zararlı içeriklere maruz kalma



Olası diğer riskler ise **dijital ayak izi** ve **bağımlılıktır**.



# Dijital Dünyanın Riskleri

## Dijital Ayak izi

- Kişilerin çevrim içi ortamlarda gerçekleştirdikleri her türlü faaliyet (paylaştığı, tıkladığı her yazı, ses, görüntü vb.) sonucu elektronik veri tabanlarında bıraktıkları ve **süresiz** olarak saklanan izdir.
- Bu izler, kişi sildiğini zannetse bile asla tam anlamıyla yok olmadıkları için gelecekte karşılıklarına çıkabilir ve zor durumda bırakabilir.





# Dijital Dünyanın Riskleri

## Dijital Ayak izi



### Çevrim içi ortamlarda bırakılan ayak izi ile:

- Bir kişinin adına, bilgisi dışında sosyal paylaşımlar yapılabilir.
- Kişinin herhangi bir konuda yaptığı bir arama işleminin konusu daha sonra reklam olarak karşısına çıkabilir.
- Kişinin paylaşmak istemeyeceği pek çok veri toplanabilir. Edinilen her bir veri ile kişinin genel profili oluşturulur. Bu verileri depolayan şirketler, verileri alıp satabilirler.
- Kişinin nelerden hoşlandığından, nerede yaşadığına kadar pek çok bilgi elde edilebilir hale gelir.

# Dijital Dünyanın Riskleri

## Teknoloji Bağımlılığı

Teknoloji bağımlılığı, teknolojiyi kullanmada ve onunla ilişkide kişinin iradesini kaybetmesi, kendini denetleyememesi ve onsuz bir yaşam sürememeye başlaması hâlidir.



# Dijital Dünyanın Riskleri

## Teknoloji Nasıl Bağımlılığa Dönüşür?



Geçirilen süre zaman içinde artış gösterir.



Kontrol ortadan kalkar ve kontrol çabaları başarısız olur.



Hareketsizliğe bağlı bedensel rahatsızlıklar ve görme problemleri ortaya çıkabilir.



Sorumluluklar yerine getirilmemeye başlanır.



Teknoloji kullanımını saklamak için yalanlar söylenir.

# Dijital Dünyanın Riskleri

## Teknoloji Nasıl Bağımlılığa Dönüşür?



Çevreden gelen yardım çabalarına yanıt verilmez, çatışma yaşanır.



Dikkat dağınıklıkları ve öfke görülebilir.



Yeme düzeni bozular.



Uyku düzeni bozular.



Duygudurum bozuklukları başlayabilir.

# İnterneti Doğru Kullanma Kılavuzu

Dijital dünyadaki risklerle baş edebilmek ve çevrim içi ortamlarda daha güvenli şekilde hareket edebilmek için bazı becerilere sahip olmalıyız.

Bu beceriler:

**Dijital vatandaşlığı** kavramak ve uygulamak,

Dijital dünyanın sorumluluklarını fark etmek,

Dijital okuryazar olabilmek,

Siber zorbalığın farkında olmak.

# Dijital Vatandaş Olmak

**Dijital vatandaş**, bilgi ve iletişim kaynaklarını kullanırken eleştirebilen, çevrim içi davranışlarının etik sonuçlarını bilen, teknolojiyi kötüye kullanmayan, dijital dünyada iletişim kurarken ve işbirliği yaparken doğru ve ahlaki davranışı teşvik eden vatandıdır.

**Dijital vatandaş**, internette ve sosyal medya platformlarında nasıl davranacağını, iletişim ve etkileşim kuracağını bilerek katılım sağlar ve tüm dünya ile bağlantıda olur.



# İyi Bir Dijital Vatandaş Olmak

Güvenli bir şekilde internette alışveriş yapma ve bankacılık hizmetlerinden yararlanma konusunda yeterli bilgiye sahip olmalısınız.

Gerçek hayatta yapmayacağınız hiçbir şeyi, çevrim içi ortamlarda da yapmamaya özen gösteriniz.



Bilgiye ulaştığınız veya gezindiğiniz siteleri, kullandığınız uygulamaları iyi tanımalısınız.

# İyi Bir Dijital Vatandaş Olmak

İnternet ortamında işlenen suçlar ve mücadele yöntemlerine karşı bilinçli olmalısınız.

İnternette yaptığınız her paylaşımın ardında silinmez izler bırakacağını unutmamalısınız. Bunu göz önünde bulundurarak çocuklarınızı ve kendinizi internetin tehlikelerinden koruyabilmelisiniz.



Dijital ortamlarda tonlamamıza dikkat etmemiz önemlidir. İletişim tonumuz yazışma dilinde istediğimiz şekilde algılanamayabilir.

Dijital ortamlarda aynı fikirde olmadığımız insanlarla sık sık karşılaşabiliriz. Böyle durumlarda empati yapmamız ve saygılı olmamız gerektiğini unutmamalıyız.



# Paylaşım yapmadan önce kendinize sorun:

- Bunu birinin suratını söyler miydiniz?
- Başka biri yazdığınız şeyi yanlış anlayabilir mi?
- Birinin adını lekeler mi?
- Birisi sizin hakkınızda böyle söylese ya da yazsa nasıl hissederdiniz?

*Çevrim içiyken size nasıl davranılmasını istiyorsanız, insanlara da öyle davranın.*



# Dijital Okuryazar Olmak

Çevrim içi ortamlarda, kontrolün sende olmasını sağlamak için **dijital okuryazar** olmak önemlidir.

**Dijital okuryazar** olmak, çevrim içi dünyadaki uygulamaları bilmek ve doğru şekilde kullanabilmek, karşısına çıkan bilgileri eleştirel şekilde analiz ederek yorumlayabilmek ve bu ortamlarda uygun içerikler oluşturabilmektir.



# Dijital Okuryazar Olmak Neden Önemli?

Dijital ortamların görünmeyen yüzü anlaşılır.



Dijital ortamlardaki hak ve sorumluluklar fark edilir.

Bilgi kirliliğinin önüne geçilir.

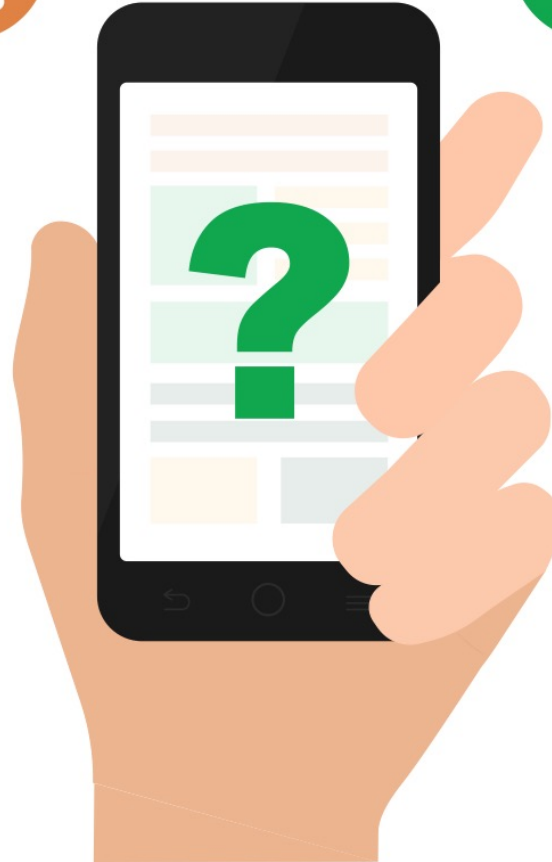


Doğru, güvenilir ve özgün içerikler oluşturur.

Sosyal medya ve diğer dijital uygulamalar kullanılırken daha bilinçli bir kullanıcı olunur.



Zorbalık, nefret söylemi gibi olumsuz durumlardan nasıl korunulacağını farkında olunur.



# Dijital Okuryazar Olmak İin:

- Doğru ve güvenli arama yöntemleri bilinmeli
- Dijital ortamlarda yaşanan sorunlarla ilgili toleranslı olunmalı
- Yenilikleri takip etme isteđine sahip olunmalı
- Dijital ortamdaki risklerin ve fırsatların farkında olunmalı
- Doğru bilgiye ulaşıldığından emin olunmalı



# Doğru Bilgiye Nasıl Ulaşırız?

Yapılan çeşitli araştırmalara göre:

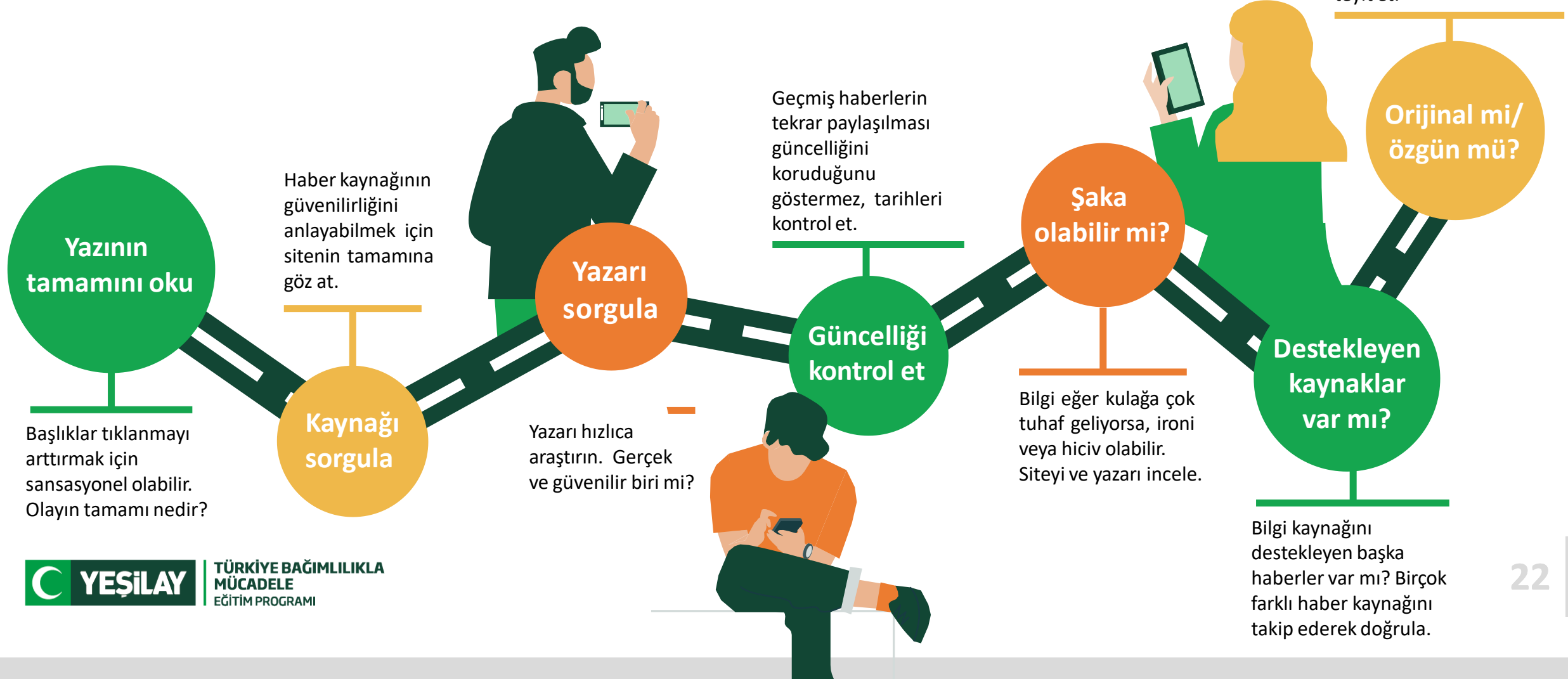
Yanlış bilgi içeren paylaşımlar, insanlara doğru bilgi içeren paylaşımlardan **6 kat** daha hızlı ulaşıyor.\*

Gerçek haberler, 1000 sosyal medya kullanıcılarından daha fazla kişiye nadiren ulaşırken yanlış bir haber rutin olarak **10 binden** fazla kişiye ulaşıyor.\*\*



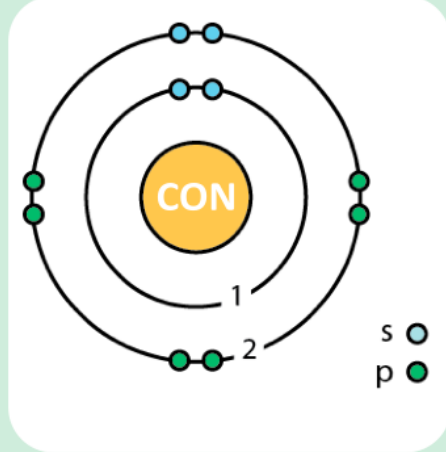
# Doğru Bilgiye Nasıl Ulaşırız?

Bir haber ile karşılaştığımızda:



# CONTORIUM ELEMENTİ

Simgesi Con, atom numarası 90, kütle numarası 367,4!  
Bu rekor bir radyoaktivite! Dünyada sadece İstanbul boğazının diplerinde bulunduğu tespit edildi!



**Türkiye'de tahmin edilen rezerv ne kadar?**

127.000 ton!

**Değeri ne kadar?**

23 trilyon dolar!

**Bütün dünya onun peşinde!**

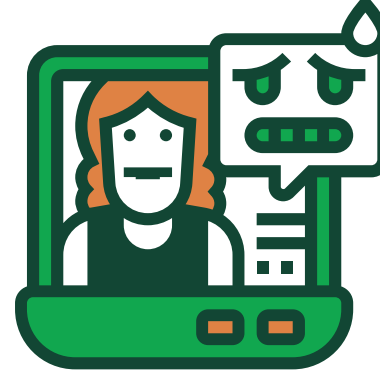
Bugün ABD, AB, bilimum Asya ülkeleri Avustralya, Antartika ve Afrika Contorium elementinin peşinde!



# Zorbalık ve Siber Zorbalık



**Zorbalık**, fiziksel veya sözlü olabilen, bir kişi ya da grup tarafından uygulanan ve çoğunlukla kişilerin kendilerine göre güçsüz ya da zayıf kişileri hedef aldığı yüz yüze, tekrarlanan, saldırgan davranışlardır.



**Siber zorbalık**, dijital teknolojilerin kullanımıyla sosyal medyada, mesajlaşma platformlarında, oyun platformlarında kişiyi korkutmayı, kızdırmayı veya utandırmayı amaçlayan, tekrarlayan zorba davranışlardır.





## ZORBALIK

Yüz yüze

Gizlenecek ya da kaçacak bir ortam bulunabilir.

Sınırlı sayıda kişi şahit olur.

Zorba tespit edilebilir.

Zorbaliğa uğrayan kişi gözle görüldüğü için empati kurulması nispeten daha kolaydır.

Zorbaliğın gerçekleştiği ortamdan uzak durulabilir.

Zorbaliğa uğrayan kişi nadiren zorbaya dönüşebilir.



## SİBER ZORBALIK

Çevrim içi

Gizlenmesi ve kaçması zordur.

Dünyanın her yerinden insana açıktır, saniyeler içinde geniş kitlelere ulaşarak popüler olabilir.

Zorba anonim olabilir.

Zorbaliğa uğrayan kişi ile empati kurmak zordur.

Zaman ve mekandan bağımsızdır.

Zorbaliğa uğrayan kişi kolayca zorbaya dönüşebilir.

# Siber Zorbalık



**Siber zorbalık konusunda şunlar örnek verilebilir:**

- Sosyal medyada birinin hakkında yalanlar yaymak veya utanç verici fotoğraflarını yayınlamak
- Mesajlaşma platformları aracılığıyla incitici mesajlar veya tehditler göndermek
- Birinin kimliğine bürünmek veya onun adına başkalarına mesajlar göndermek

# Zorbalığın «Siberini» Nasıl Tanırız ?

- Elektronik cihazlar ve teknolojinin kullanılması
- Zarar verme/ incitme isteđi
- Güç dengesinde eşitsizlik
- Tekrarlayıcı olması
- Anonim kişi ya da kişilerden gelmesi
- Açık ve görülebilir şekilde olması veya gizli bir şekilde gerçekleşmesi



# Siber Zorbalık Türleri



# Siber Zorbanın Özellikleri

- Yüz yüze iletişimde çoğunlukla zorlanır.
- Akademik başarısı genellikle düşüktür.
- Zihinsel ve duygusal olarak çoğunlukla güçsüzdür.
- Öfkeyi uygun bir şekilde nasıl ifade edeceğini bilemeyebilir.
- Birine çevrim içi ortamda söylediklerini o kişinin yüzüne söylemesi pek olası değildir (özellikle buna şahit olacak bir arkadaş ya da yetişkin varsa).
- Genellikle eylemlerinin sorumluluğunu almaz.



# Neden Siber Zorbalık Yapılır?

- Öfke
- İntikam
- Hayal Kırıklığı
- Eğlence
- Etkileşim İsteği
- Güç Arzusu

Tüm zorbaları zorba davranışları için motive eden etkenler farklı olduğu gibi, zorbalığı ortadan kaldıracak çözüm ve tepkiler de farklı olacaktır.



# Siber Zorbaliđa Uđrarsam Ne Yapabilirim?

- Zorbaliđa uđradıđınızı dűşünüyorsanız, öncelikle çaresiz olmadıđınızı bilin. İlk adım olarak güvendiđiniz birinden veya resmi kurumlardan yardım isteyebilirsiniz.
- Zorbalık sosyal bir platformda gerçekleşiyorsa, zorbayı hemen engellemeyi ve davranışlarını sosyal medya platformunun kendisine resmi olarak bildirmeyi ihmal etmeyin. Sosyal medya şirketleri, kullanıcılarını güvende tutmakla yükümlüdür ve gerekirse yaptırım uygulayabilirler.



# Siber Zorbaliđa Uđrarsam Ne Yapabilirim?

- Gerektiđinde kullanmak üzere rahatsız edici ieriklerin görüntülerini alarak kanıt toplayabilirsiniz. Yasal haklarınızı kullanırken bu kanıtlar faydalı olabilir.
- Zorbaliđın toplumsal olarak önlenmesi bireysel mađduriyetlerin bildirilmesine bađlıdır. Zorbaliđı bildirerek zorbaya davranışının yanlış ve cezaya tabii olduđunu da göstermiş oluruz.
- Acil bir tehlike içindeyseniz (sürekli aranarak rahatsız ediliyorsanız, konumunuz takip ediliyorsa vb.) polise başvurabilirsiniz.





# Hukuki Boyut

Kişi ve kurumların hak ve sorumlulukları:

«5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun»

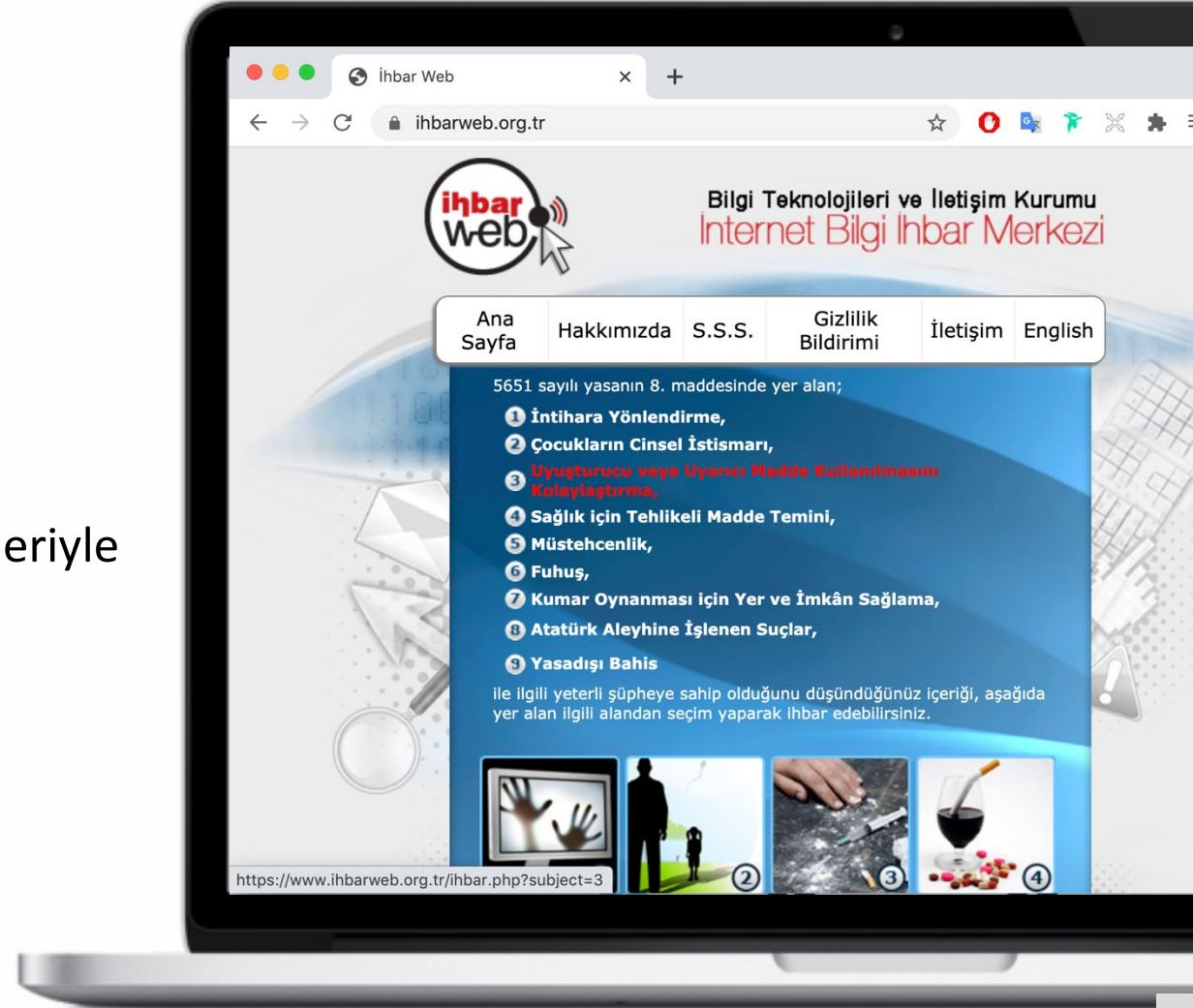
ile belirlenmiştir.



# Hukuki Boyut

Türk Ceza Kanununda yer alan:

- İntihara yönlendirme,
  - Çocukların cinsel istismarı,
  - Sağlık için tehlikeli madde temini,
  - Müstehcenlik
  - Kumar oynanması için yer ve imkân sağlama
- gibi suçlardan biri veya birkaçını barındıran internet siteleriyle ilgili [www.ihbarweb.org.tr](http://www.ihbarweb.org.tr) adresinden şikâyet gerçekleştirebilirsiniz.



# Hukuki Boyut

İnternet üzerinden bir suç ile karşılaşıldığında:

[www.ihbarweb.org.tr](http://www.ihbarweb.org.tr) adresinden şikayet gerçekleştirilebilir.

**İNTİHARA YÖNLENDİRME ve TEŞVİK ETME**

**Emniyet İhbar Hattı:**

<https://onlineislemler.egm.gov.tr/Sayfalar/Ihbar.aspx>

**ÇOCUKLARIN CİNSEL İSTİSMARINA  
YÖNELİK İÇERİKLER**

**Aile, Çalışma ve Sosyal Hizmetler Bakanlığının Alo 183 Sosyal Destek Hattı:**

<http://alo183.gov.tr/>

**Emniyet İhbar Hattı:** <https://onlineislemler.egm.gov.tr/Sayfalar/Ihbar.aspx>

**MÜHTEHCEN ve PORNOGRAFIK İÇERİKLER**

**Emniyet İhbar Hattı:**

<https://onlineislemler.egm.gov.tr/Sayfalar/Ihbar.aspx>

**SAĞLIK İÇİN TEHLİKELİ OLABİLECEĞİ  
DÜŞÜNÜLEN ÜRÜNLER**

**Emniyet İhbar Hattı:** <https://onlineislemler.egm.gov.tr/Sayfalar/Ihbar.aspx>

**Türkiye Eczacılar Birliği İnternet Üzerinden Satış Bildirimi:**

<https://tebapp.tebeczane.net/internet-uzerinden-satis-bildirimi>

# İnterneti Güvenli Kullanım İin İpuları



İnternette veya sosyal medya hesaplarınızda kişisel bilgilerinizi paylaşmamaya özen gösterin.



Kırıcı yorumları, mesajları ve fotoğrafları bildirebilir ve bunların kaldırılmasını isteyebilirsiniz.



Hibir sosyal medya uygulaması, insanlara onları engellediğinizde, kısıtladığınızda veya şikayet ettiğinizde bildirim göndermez ve haberdar etmez.

# İnterneti Güvenli Kullanım İin İpuları



Kullandığınız Őifrelerin sadece sizin anlayabileceğiniz, tahmin edilmesi zor ve güçlü Őifreler olabilmeleri için sayı, harf ve sembolleri birlikte kullanınız. Bilgilerinizin güvenlięi için belirli aralıklarla tüm Őifrelerinizi deęiřtirmeye alışınız.



Akıllı telefonunuza indirdięiniz uygulamaları onaylamadan önce telefonunuzdaki hangi kiřisel bilgilere ve uygulamalara eriřim istedięini kontrol ediniz.



Akıllı telefonunuzda bulunan uygulama marketlerinin izin vermedięi, güvenli olmayan uygulamaları indirmeyiniz.

# İnterneti Güvenli Kullanım İin İpuları



Kullanılan teknolojik cihazlardaki (akıllı telefon, tablet, vb.) ve bu cihazlarda kullanılan uygulamalardaki gizlilik ayarlarını kontrol edin. Gizlilik politikaları gncellendiğinde, onay vermeden nce gz atmak, uygulamanın ne tr bilgilerinize ulařacađını bilmek aısından faydalı olabilir.



cretsiz uygulamaların (sosyal medya platformları dahil) size bu hizmetleri bilgileriniz karřılıđında sađladığını unutmayın.

# İnterneti Güvenli Kullanım İin İpuları



Başka birinin hazırladığı içeriği paylaşmadan önce, bu içeriğin kaynağının ne olduğunu, kimin hazırladığını, nerede ve ne zaman hazırladığını araştırın. Paylaştığınız içerik gerçek olmayabilir.



Artık kullanmadığınız hesaplarınızı silin veya devre dışı bırakın. Eğer öylece bırakırsanız haberiniz bile olmadan ele geçirilmesi olasıdır.



# İNTERNETİN GÜVENLİ KULLANIMI ve SİBER ZORBALIK

Teşekkür ederiz



TÜRKİYE BAĞIMLILIKLA  
MÜCADELE  
EĞİTİM PROGRAMI

[tbm.org.tr](http://tbm.org.tr)