



# İNTERNETİN GÜVENLİ KULLANIMI ve SİBER ZORBALIK



TÜRKİYE BAĞIMLILIKLA  
MÜCADELE  
EĞİTİM PROGRAMI

LİSE

# Sunum İeriđi

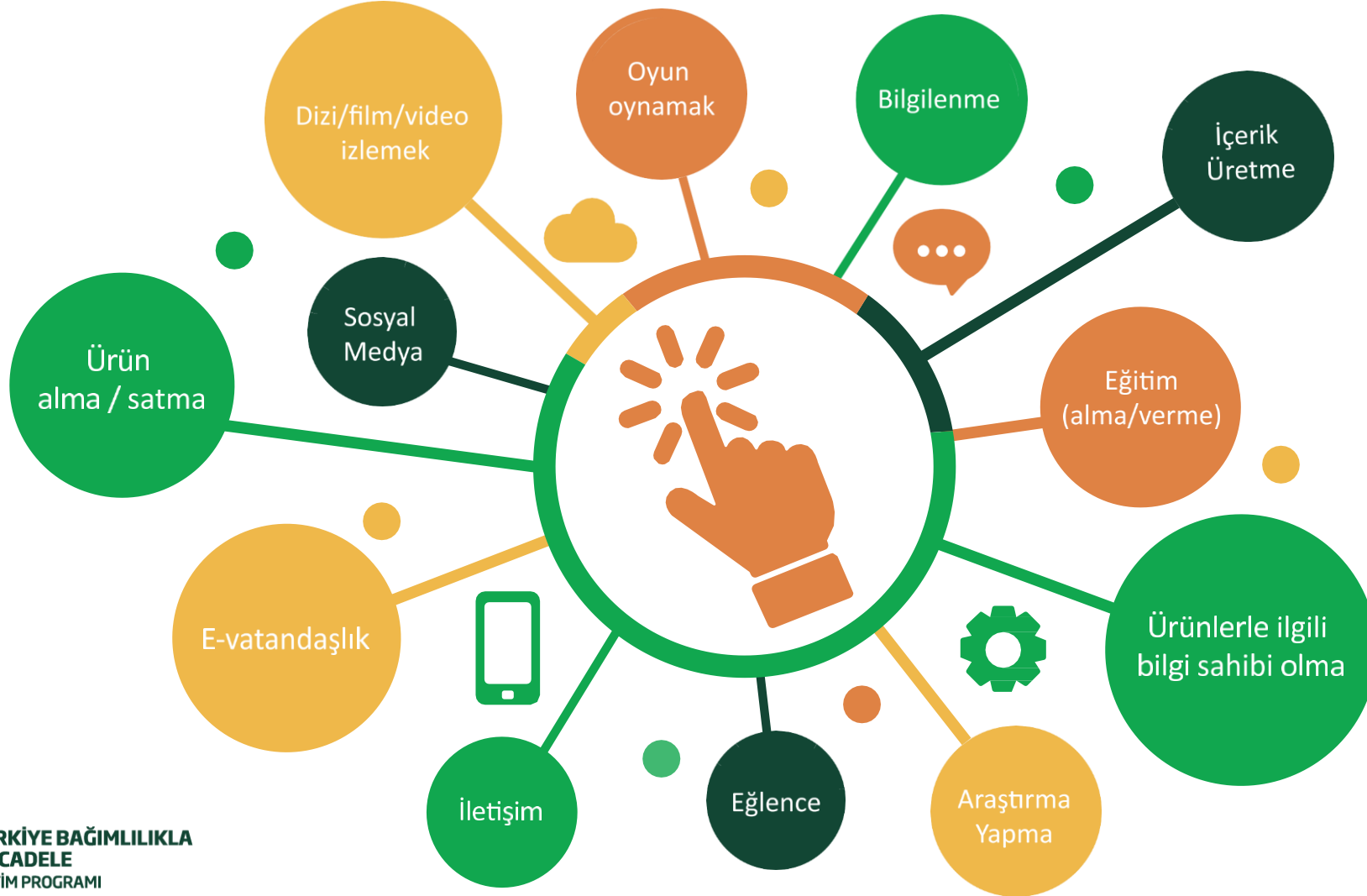
- İnternet ile Neler Yapabiliriz?
- Dijital D nyanın Riskleri
- Dijital Vatandař Olmak
- Dijital D nyada Sorumlu Davranmak İin
- Dijital Okuryazarlık
- Siber Zorbalık
- Hukuki Boyut
- İnterneti G venli Kullanım İin İpuları



# İnternet ile Neler Yapabiliriz?



# İnternet ile Neler Yapabiliriz?



# İnternet: Yararlı mı? Zararlı mı?

İnternetin birçok farklı kullanım alanı vardır. Güvenli ve doğru bir şekilde kullandığımızda bu kullanım alanları bize pek çok fayda sağlar. Uygun sınırlarda kullanmadığımızda ise bazı risklerle karşılaşabiliriz.



# 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, gizliliğin ihlal edilmesi



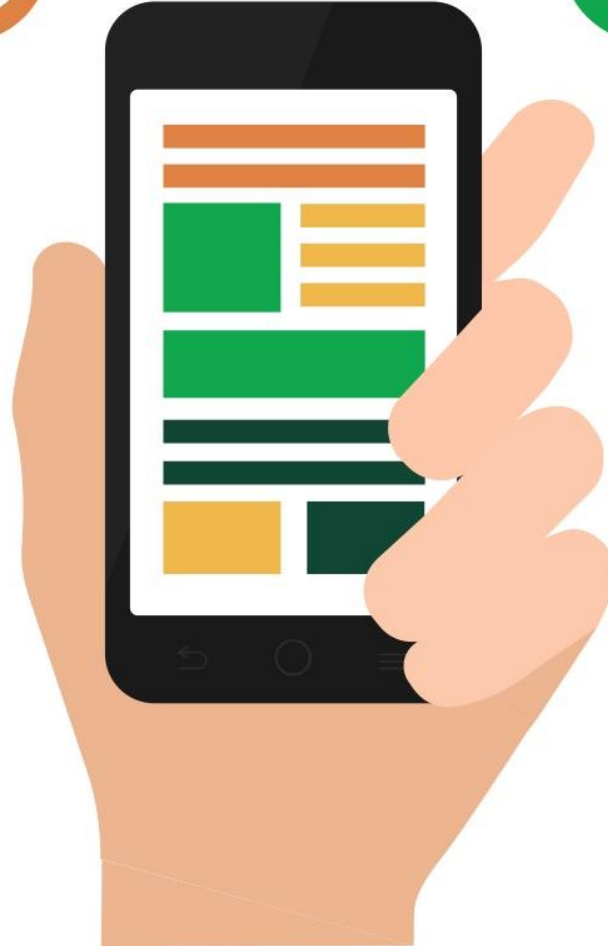
**Ticari Riskler:** Aşırı veya gizli pazarlama, dolandırıcılık vb.



**İçerik Riskleri:** Zararlı, rahatsız edici (şiddet içerikli, cinsiyete yönelik ayrımcılık içeren, saldırgan, uygunsuz içerik vb.) içeriklere maruz kalabilirsin.



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



# Dijital Dünyanın Riskleri

## Dijital Ayak izi

Çevrimiçi ortamda kişinin bıraktığı, paylaştığı, tıkladığı her yazı, ses, görüntü, bilgi sonucu ortaya çıkan **süresiz** izlerdir.

Çevrimiçi ortamlarda yaptığınız her paylaşımın ardında **silinmez** izler bırakacağını unutmamalısınız.

Bu izler, sildiğimizi zannetsek bile asla tam anlamıyla yok olmadıkları için gelecekte karşımıza çıkabilir ve bizi zor durumda bırakabilir.



# Dijital Dünyanın Riskleri

## Dijital Ayak izi

Örneğin:



- Herhangi bir konuda yapılan arama işlemlerinin daha sonra kişinin karşısına reklam olarak çıkması
- Gizli tutulan profillerin ve paylaşımların açığa çıkarılması
- Teknoloji firmalarının, kişinin nelerden hoşlandığından, nerede yaşadığına kadar pek çok bilgiyi algoritmaları sayesinde elde etmesi
- Toplanan bu bilgilerin güvenlik açıkları yüzünden sızdırılabilmesi ve kötü niyetli kişilerin eline kolaylıkla geçebilmesi



# 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?

**Teknolojik cihazlarda ve internet tabanlı uygulamalarda:**



Geçirilen sürenin zaman içerisinde artış göstermesi



Negatif etkilerine rağmen yoğun kullanımı sürdürme



Kullanmayı azaltmak isteme ama bırakamama



Sosyal ilişkilerin, kişisel etkinliklerin yerini almaya başlaması

**durumlarında bağımlılık akla gelir ve profesyonel destek almak gerekebilir.**

# İnterneti Doğru Kullanma Kılavuzu

Dijital dünyadaki risklerle baş edebilmek, çevrimiçi 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 Olabiliriz

*Dijital vatandaşlık*, çevrimiçi dünyada nasıl bir tavır içinde olmamız gerektiğini tanımlayan kavramdır.

Çevrimiçi ortamda sorumlu ve uygun davranmak için *dijital vatandaş* olmamız çok önemlidir.



*Dijital vatandaş*, internette ve sosyal medya platformlarında nasıl davranacağını, iletişim kuracağını bilir ve tüm dünya ile bağlantıda olur.

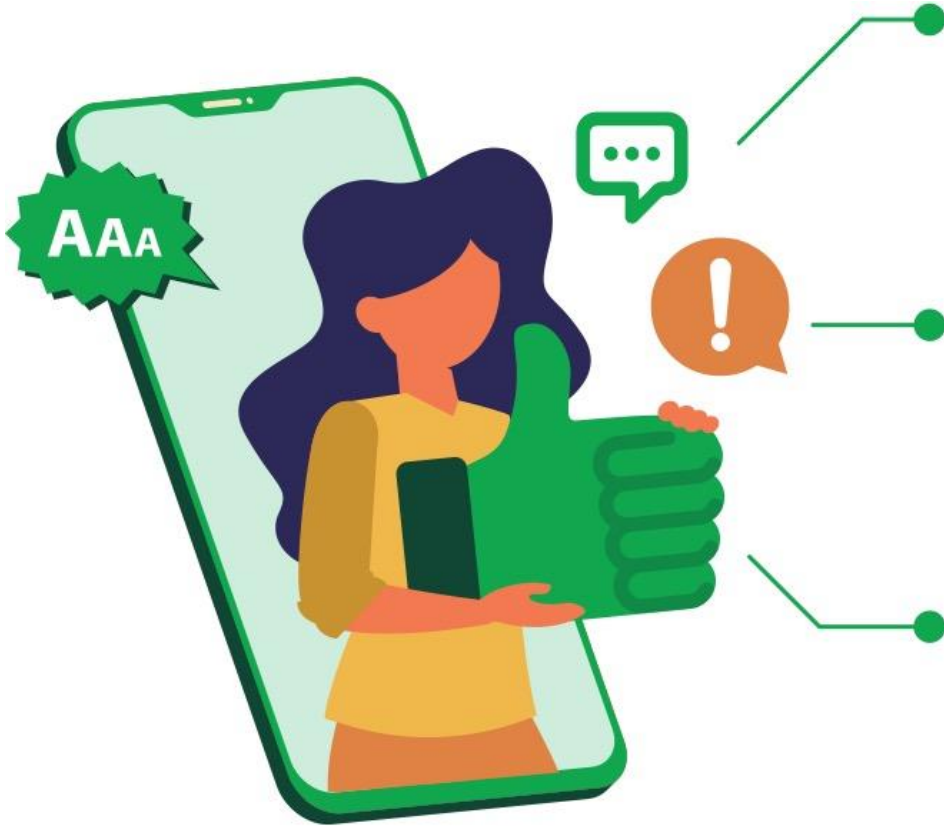
# Dijital Vatandaş Olabiliriz

Çevrimiçi ortamlarda da sorumluluklarımızın farkında olmalıyız. Davranışlarımızın etik, yani uygun ve sorumlu bir çerçevede nasıl uygulanacağı ile ilgili farkındalık sahibi olmalıyız.



Dijital ortamdaki her bir davranışımız bizim dijital itibarımızı etkiler. Bu yüzden sorumluluk sahibi olmamız ve başkalarının haklarına saygılı davranmamız çok önemlidir.

# Dijital Dünyada Sorumlu Davranmalıyız



Dijital ortamlarda yazışarak iletişim kurarken, mesajın istediğin gibi anlaşılmayabilir, iletişim tonuna dikkat etmelisin.

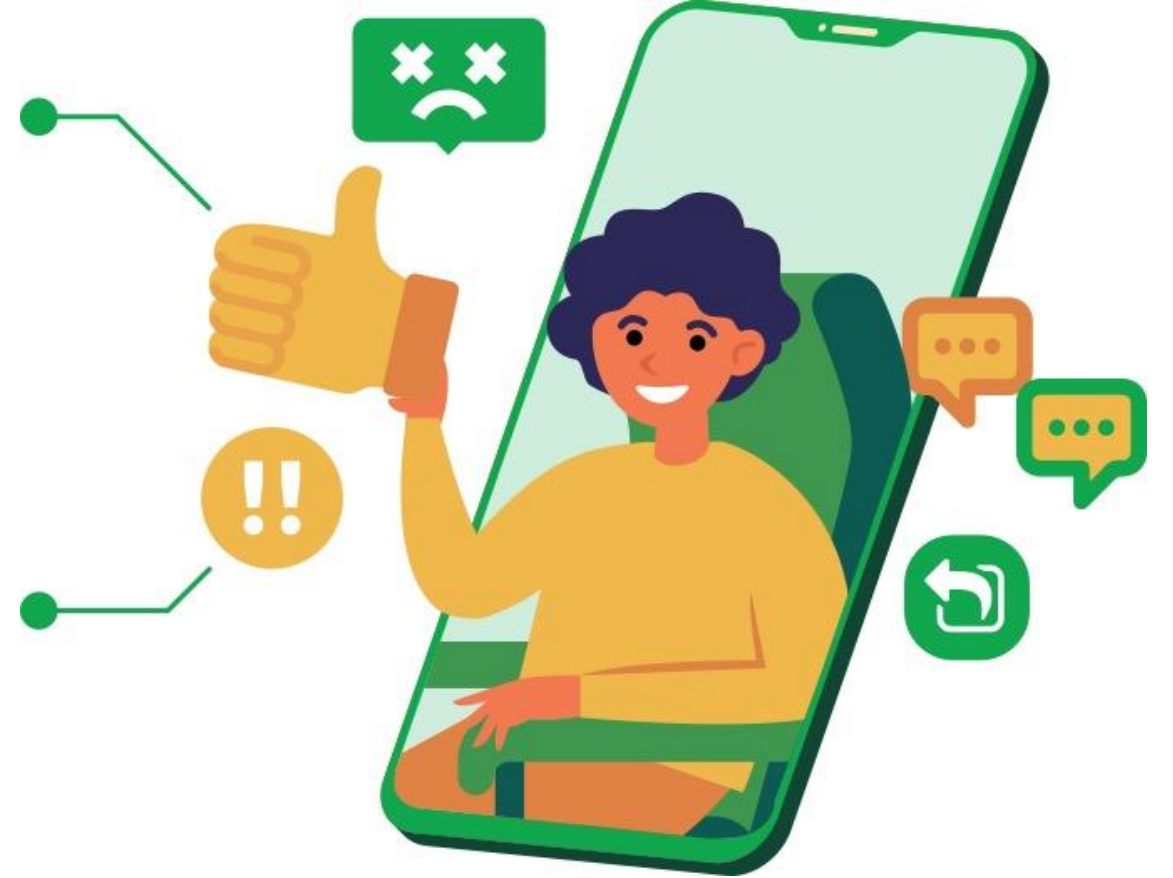
Yazışma dilinde gereksiz büyük harf kullanmak, karşındaki insanların onlara bağırıldığını düşünmelerine sebep olabilir.

Herhangi bir platformda görüş bildirirken tıpkı gerçek hayatta olduğu gibi saygılı ve nazik olmalısın.

# Dijital Dünyada Sorumlu Davranmalıyız

Dijital ortamlarda farklı fikirdeki insanlarla karşılaştığında, tartışmalarda üslubuna dikkat etmeli, öfkeli ve saygısız ifadeler kullanmamalısın.

İnternetteki bir bilginin herkese açık olması, onu izinsiz kullanabileceğimizi göstermez. Bilgi hırsızlığından kaçınmak için aldığın her bilginin kaynağını belirtmelisin.



# Dijital Dünyada Sorumlu Davranmalıyız



Dijital araçları kullanırken başkalarına zarar vermekten de özenle kaçınmalısın.

Gerçek hayatta yapmayacağın hiçbir şeyi, internetten de yapmamalısın.

Bir paylaşımı okuduktan sonra rahatsız olduğunu hissediyorsan hemen tepki vermemelisin. Anlık olumsuz tepkiler hiç istemeyeceğin sonuçlar doğurabilir.



# Dijital Okuryazar Olmak

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

**Dijital okuryazar** olmak:

- Çevrimiçi dünyadaki uygulamaları bilmek,
- Onları doğru şekilde kullanabilmek,
- Karşılaşılan bilgileri eleştirel şekilde analiz ederek yorumlayabilmek,
- Dijital ortamlarda uygun içerikler oluşturabilmeyi kapsamaktadır.



# Dijital Okuryazar Olmak Neden Önemli?

Dijital ortamların görünmeyen yüzü anlaşılır.



Bilgi kirliliğinin önüne geçilir.



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



Dijital ortamlardaki hak ve sorumluluklar fark edilir.



Doğru, güvenilir ve özgün içerikler oluşturur.

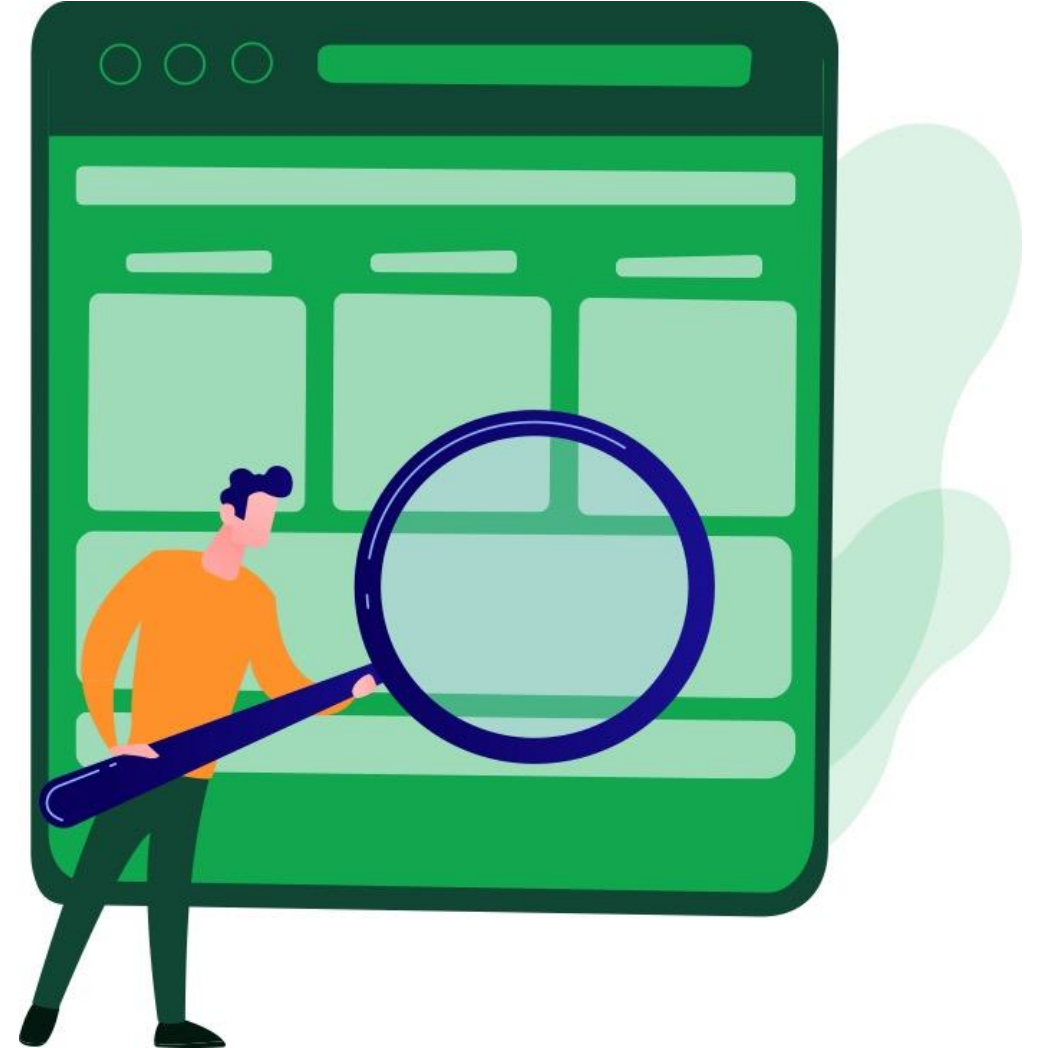


Zorbalık, nefret söylemi gibi olumsuz durumlardan nasıl korunulacağının farkında olunur.



# Dijital Okuryazar Olmak İin:

- Doğru ve güvenli arama yöntemleri bilinmeli
- Dijital ortamlarda yaşanan sorunlarla ilgili toleranslı olunmalı
- Dijital ortamdaki risklerin ve fırsatların farkında olunmalı
- Karşılaşılan her içeriğē eleştirel bir gözle bakılmalı
- 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.\*\*

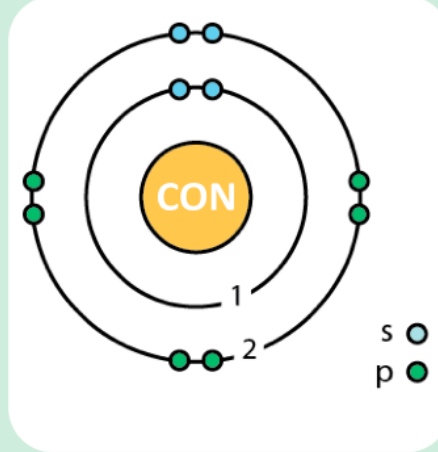


# Doğru Bilgiye Nasıl Ulaşırız?



# 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!

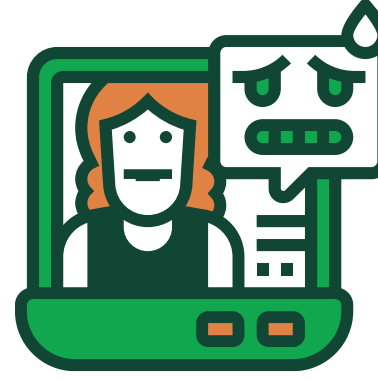
**Bütün dünya onun peşinde!**

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.

Kurban gözle görüldüğü için empati kurması nispeten daha kolaydır.

Zorbalığın gerçekleştiği ortamdan uzak durulabilir.

Kurban nadiren zorbaya dönüşebilir.



## SİBER ZORBALIK

Çevrimiçi

Gizlenmesi ve kaçması zordur.

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

Zorba anonim olabilir.

Kurban ile empati kurmak zordur.

Zaman ve mekandan bağımsızdır.

Kurban kolayca zorbaya dönüşebilir.



# Siber Zorbalık



- 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?



# Şaka mı, Zorbalık mı?

- Tüm arkadaşlar birbirleriyle şakalaşır. Ancak seni üzen bir şaka durmasını istemene rağmen devam ediyorsa ve senin için artık eğlenceli değilse, bu zorbalık olabilir.
- Zorbalık çevrimiçi gerçekleştiğinde, hiç tanımadığınız insanlar dahil geniş kitlelere ulaşabilir ve istenmeyen bir ilgiye neden olabilir. İçinde bulunduğun durumun seni üzdüğünü ve artık dozunu aştığını düşünüyorsan buna bir dur diyebilirsin.



# Paylaşım yapmadan önce kendine sor:

- Bunu birinin yüzüne de söyler miydin?
- Başka biri yazdığın şeyi yanlış anlayabilir mi?
- Birinin itibarını zedeler mi?
- Biri senin hakkında böyle söylese ya da yazsa nasıl hissederdin?
- Arkadaşlarının, ailenin ve öğretmenlerinin yazdığın bu tür şeyleri okumasını ister miydin?

**Çevrimiçiyken sana nasıl davranılmasını istiyorsan sen de insanlara öyle davran.**



# Siber Zorbalık Türleri

**Dışlama:** Kasıtlı olarak belli kişi ya da kişileri çevrimiçi grupların, etkinliklerin ve oyunların dışında bırakmaktır.

**Kişiliğe Bürünme:** Başkasının kimlik bilgilerini çalmak, resim göndermek veya sahte sosyal medya hesapları oluşturmak yoluyla zorbalığa maruz bırakılabilirsiniz. Bu tür bir kişi, sizin ya da ailenizin diğer fertlerinin çevrimiçi ortamda yaptığı paylaşımları takip ederek, inandırıcı sahte bir kimlik oluşturabilir.



# Siber Zorbalık Türleri

**İfşa:** Bir kişiyi veya bir grubu, onlarla ilgili hassas veya özel bilgileri rızaları olmaksızın çevrimiçi ortamda yayınlayarak utandırmak veya alenen aşağılamak anlamına gelir. Kişinin rızası ve haberi olmadığından, bu tür paylaşımların yasal sonuçları oldukça ciddidir.

**Karalama/Linç Etme ve Dedikodu Üretme:** Bir kişinin itibarına zarar verecek dedikodular veya söylentiler üreterek yaymaktır. Hızlı ve kontrolsüz bir şekilde yayılan bu söylentiler kişinin sosyal hayattan izole olmasına yol açabilir.



# Siber Zorbalık Türleri

**Çevrimiçi Taciz:** Taciz, zorbalığın en ciddi biçimlerinden biridir. Mağdura yönelik taciz, zalimce ve tehdit edici mesajlarla kendini gösterir. İsim takma, alay etme, iftira atma, fiziksel görünüş ile ilgili acımasız yorumlar yapma ve aşağılama gibi davranışlar örnek olarak verilebilir. Dramatik ve hiç beklenmedik durumlara yol açabilir.





# Siber Zorbanın Özellikleri

- Yüz yüze iletişimde çoğunlukla zorlanır.
- Okul başarısı genellikle düşüktür.
- Öfke, üzüntü, hayal kırıklığı gibi duygularını anlamakta ve düzenlemekte zorlanır.
- Birine çevrimiçi ortamda söylediklerini o kişinin yüzüne söylemesi pek olası değildir (özellikle buna şahit olacak bir arkadaş, ebeveyn veya öğretmen varsa).





# Siber Zorbalığa Uğramanın Kişiyeye Etkileri



## ZİHİNSEL ETKİLER

sevdiği şeylere karşı  
ilgisini kaybetmesi



## DUYGUSAL ETKİLER

- üzgün
- utanmış
- sersemlemiş
- kızgın hissetmek



## FİZİKSEL ETKİLER

yorgunluk  
uykusuzluk  
mide ağrısı  
baş ağrısı

# Siber Zorbalığın Etkileri

Siber zorbalığa uğradığınızda tehlikede olduğunuzu ve çözüm yolu bulamayacağınızı düşünebilirsiniz. Kişi üzerinde birçok farklı etkiye neden olabilir ve uzun sürebilir. Ancak bunların üstesinden gelinebilir ve insanlar güvenlerini ve sağlıklarını yeniden kazanabilirler.



# Siber Zorbalığa Uğrarsam Ne Yapabilirim?

- Zorbalığa uğradığını düşünüyorsan, öncelikle çaresiz olmadığını bil. İlk adım olarak sana yardım edebileceğini düşündüğün bir yetişkinden yardım isteyebilirsin.
- Okulunda bulunan psikolojik danışmana veya sevdiğin bir öğretmene ulaşabilirsin.
- Zorbalık sosyal bir platformda gerçekleşiyorsa, zorbayı hemen engellemeyi ve davranışlarını sosyal medya platformunun kendisine de resmi olarak bildirmeyi ihmal etme.



# Siber Zorbalięa Uęrsam Ne Yapabilirim?

- Gerektięinde kullanmak üzere rahatsız edici ieriklerin grntlerini alarak kanıt toplayabilirsin. Yasal haklarını kullanırken bu kanıtlar faydalı olabilir.
- Zorbalięın toplumsal olarak nlenmesi bireysel maęduriyetlerin bildirilmesine baęlıdır. Zorbalięı bildirerek zorbaya davranışının yanlış ve cezaya tabii olduęunu da gstermiř oluruz.
- Acil bir tehlike iindeyseniz (srekli aranarak rahatsız ediliyorsanız, konumunuz takip ediliyorsa vb.) polise bařvurabilirsiniz.



# Hukuki Boyut

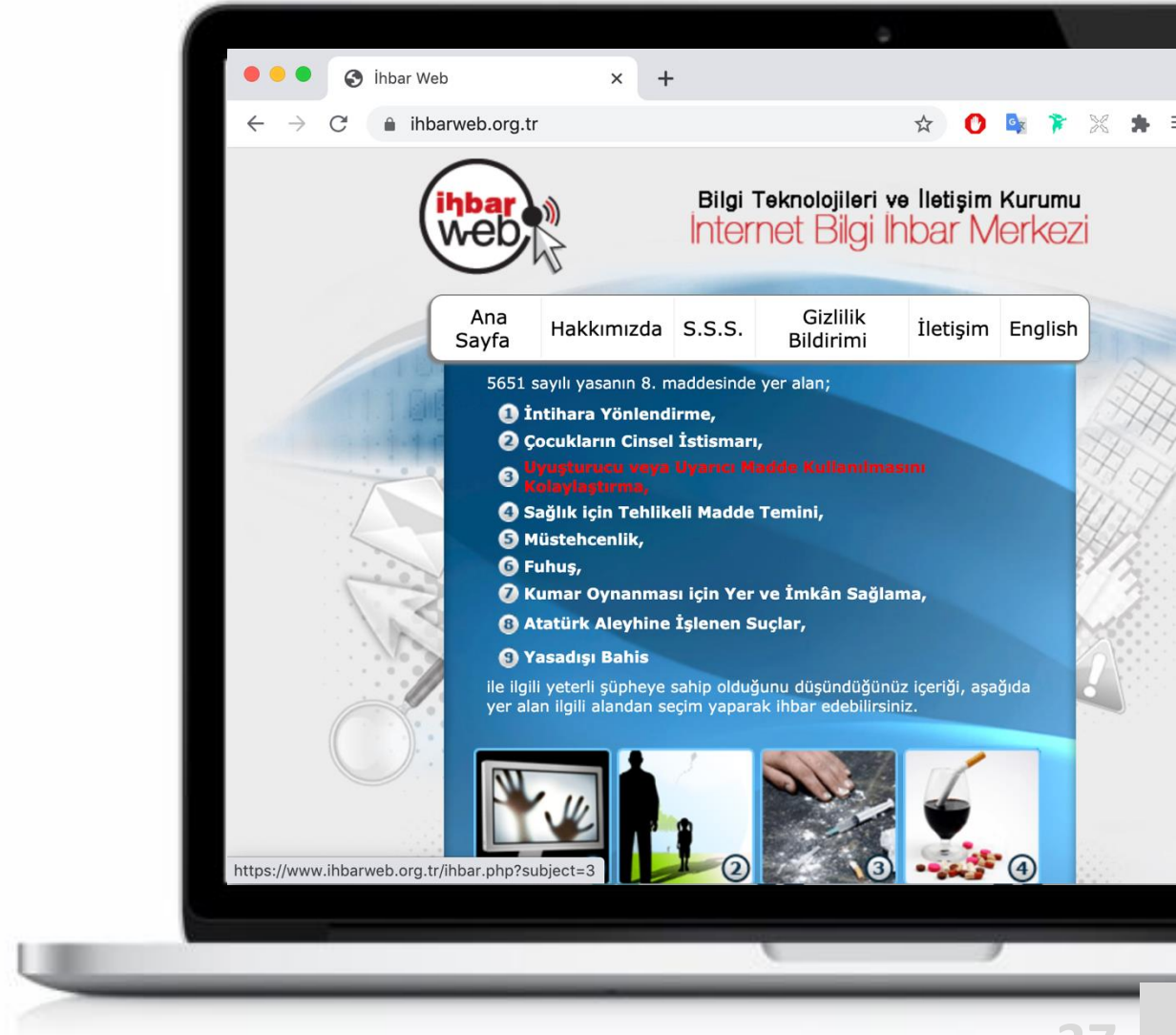
Türk Ceza Kanununda yer alan:

- 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.



# İnterneti Güvenli Kullanım İçin İpuçları



İnternette veya sosyal medya hesaplarında kişisel bilgilerini (T.C. kimlik no, telefon, adres, yaş, aile bilgileri vb.) hiçbir şekilde paylaşmamalısın.



Kullandığın şifrelerin sadece senin anlayabileceğin güçlü şifreler olabilmesi için sayı, harf ve sembolleri birlikte kullanmaya çalışabilirsin.



Dosya ya da program indirme gibi işlemleri bilinen ve güvenli internet sitelerinden yapabilirsin. Tanımadığın kişilerden ya da internet sitelerinden gelen mesajları açma ve linkleri tıklamadığından emin ol.

# İnterneti Güvenli Kullanım İçin İpuçları



Hesap gizlilik ayarlarını değiştirerek kimlerin profilini görebileceğine, sana doğrudan mesaj gönderebileceğine veya gönderilerine yorum yapabileceğine karar verebilirsin.



İnternette veya sosyal medyada yeni arkadaşlar edinirken dikkatli ol. Tanımadığın kişiler arkadaşlık teklifinde bulunduğunda kabul etmemek daha güvenli olacaktır.

# İnterneti Güvenli Kullanım İçin İpuçları



Halka açık ya da bilmediğin alanlardaki wifi ağları tehlikeli olabilir. Bu ağlar kişisel bilgilerini çalmak için oluşturulmuş sahte bağlantılar olabilir.



Bluetooth veya Airdrop'u kullanmadığın zaman devre dışı bırak. Bu bağlantı birçok cihazın birbiri ile etkileşim halinde bulunmasına olanak sağlar ve bir hacker bu açık Bluetooth bağlantıları içinden cihazına erişim sağlayabilir.



Cep telefonunda bulunan uygulama marketlerinin izin vermediği, güvenli olmayan uygulamaları indirme.



# İnterneti Güvenli Kullanım İçin İpuçları



Herhangi bir içerik paylaşmadan önce dur ve bu içerik ile biri sana zarar verebilir mi, sen başkasına zarar verir misin diye iyice düşün.



Paylaştığın fotoğrafların / videoların kötü niyetli insanlar tarafından değiştirilebileceğini unutma. Bu yüzden paylaştığın fotoğrafları seçerken dikkatli ol.



Artık kullanmadığın hesaplarını sil veya devre dışı bırak. Eğer öylece bırakırsan haberin bile olmadan ele geçirilebilir.

# İNTERNETİN GÜVENLİ KULLANIMI ve SİBER ZORBALIK

Teşekkür ederiz

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



TÜRKİYE BAĞIMLILIKLA  
MÜCADELE  
EĞİTİM PROGRAMI