



# İNTERNETİN GÜVENLİ KULLANIMI ve SİBER ZORBALIK



**YEŞİLAY**

**TÜRKİYE BAĞIMLILIKLA  
MÜCADELE  
EĞİTİM PROGRAMI**

**LİSE**

# Sunum İeriđi

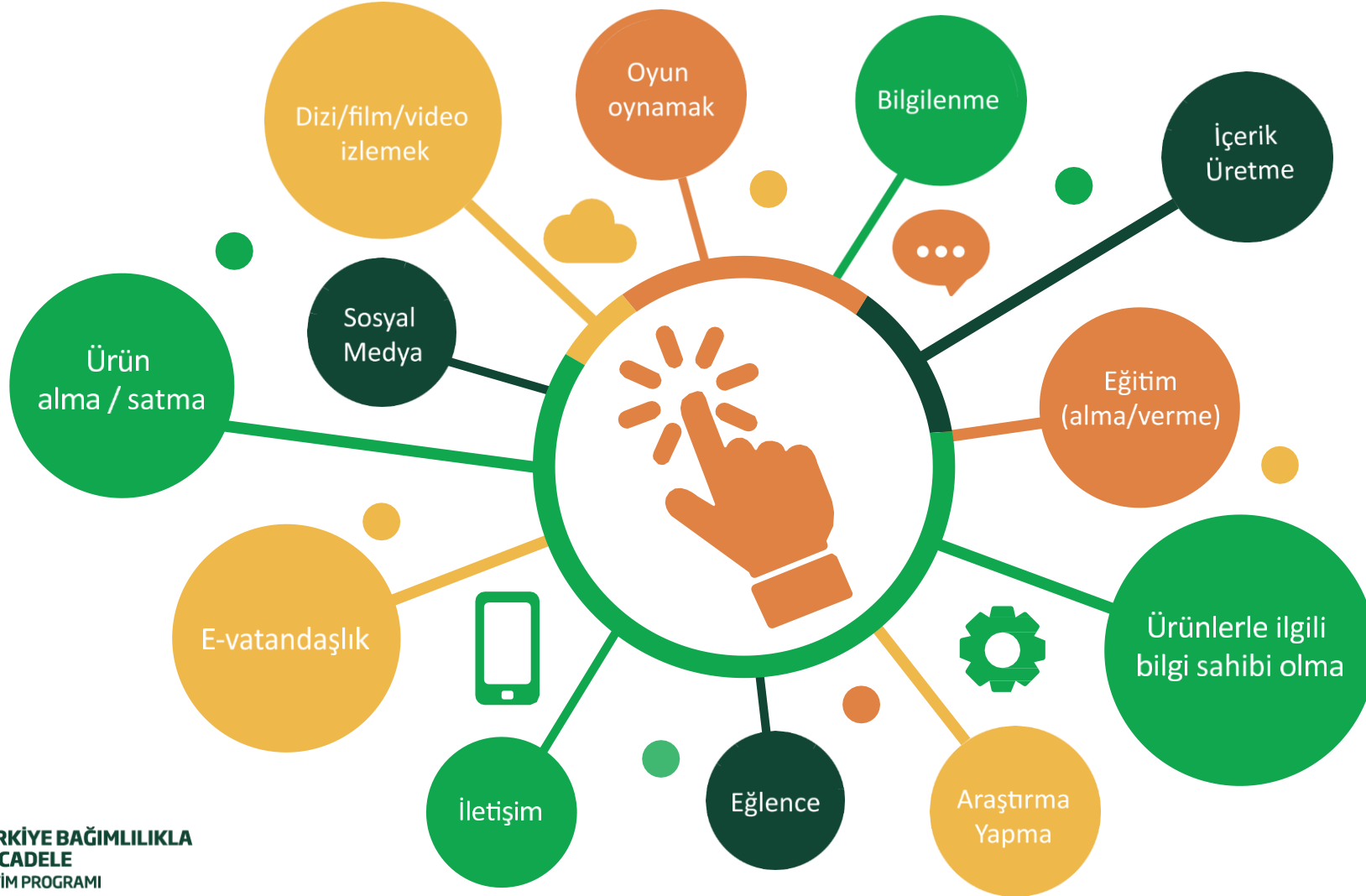
- İnternet ile Neler Yapabiliriz?
- Dijital Dnyanın Riskleri
- Dijital Vatandař Olmak
- Dijital Dnyada Sorumlu Davranmak İin
- Dijital Okuryazarlık
- Siber Zorbalık
- Hukuki Boyut
- İnterneti Gvenli Kullanım İin İpuları



# 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



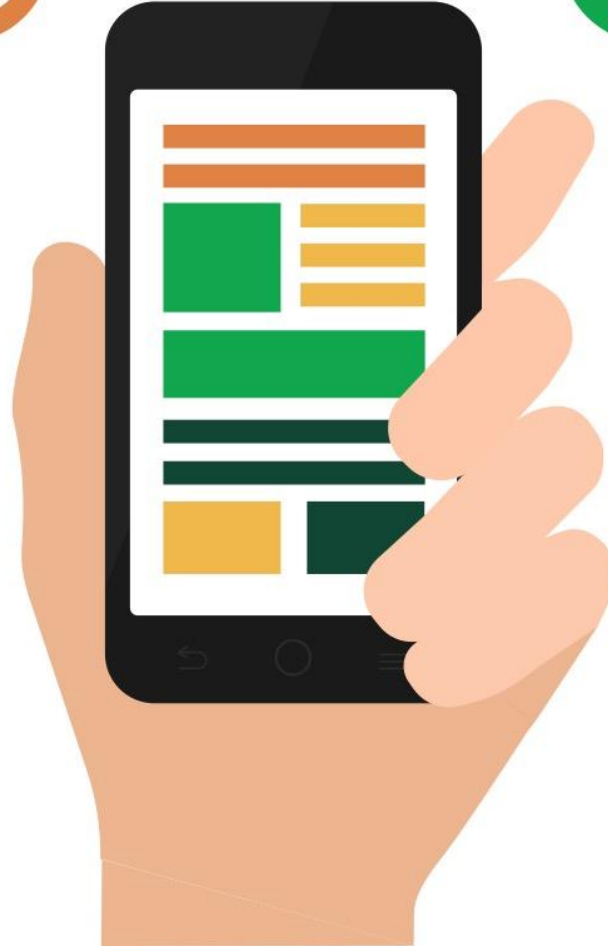
**Ticari Riskler:** Aşırı veya gizli pazarlama, dolandırıcılık vb.



**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

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

Çevrim içi 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 elde edebilmesi
- 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?



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, 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 Olabiliriz

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

Çevrim içi 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

Çevrim içi 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 bağırdığını düşünmelerine sebep olabilir.

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





# 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

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

**Dijital okuryazar** olmak:

- Çevrim içi 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.

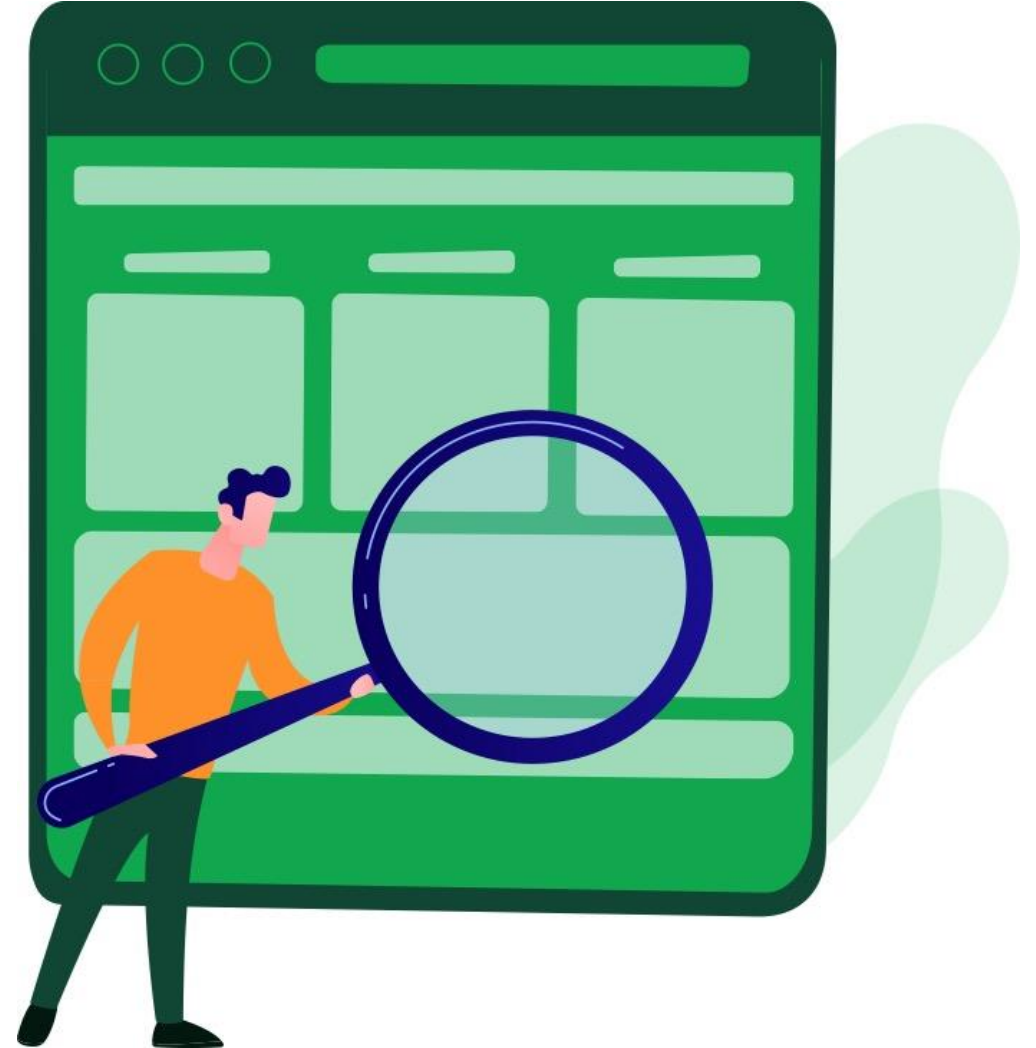


Zorbalık, nefret söylemi gibi olumsuz durumlardan nasıl korunulacağına farkında olunur.



# Dijital Okuryazar Olmak İin:

- Dođru ve gvenli arama yntemleri bilinmeli
- Dijital ortamlarda yařanan sorunlarla ilgili toleranslı olunmalı
- Dijital ortamdaki risklerin ve fırsatların farkında olunmalı
- Karřılařılan her ieriđe eleřtirel bir gzle bakılmalı
- Dođru bilgiye ulařıldıđından emin olunmalı



# Dođru Bilgiye Nasıl Ulařırız?

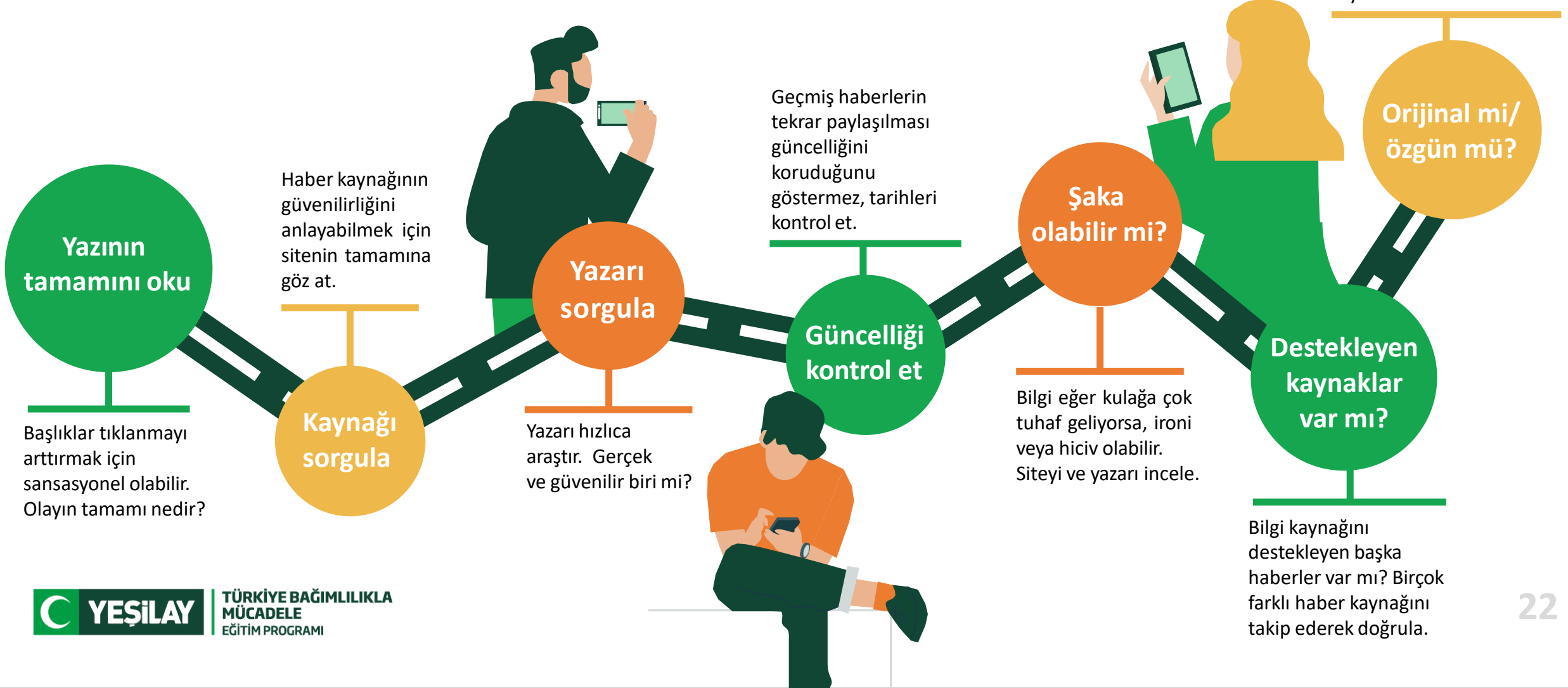
Yapılan çeřitli arařtırmalara göre:

Yanlıř bilgi ieren paylařımlar insanlara dođru bilgi ieren paylařımlardan **6 kat** daha hızlı ulařıyor.\*

Gerek haberler, 1000 sosyal medya kullanicısından daha fazla kiřiye nadiren ulařırken yanlıř bir haber rutin olarak **10 binden** fazla kiřiye ulařıyor.\*\*

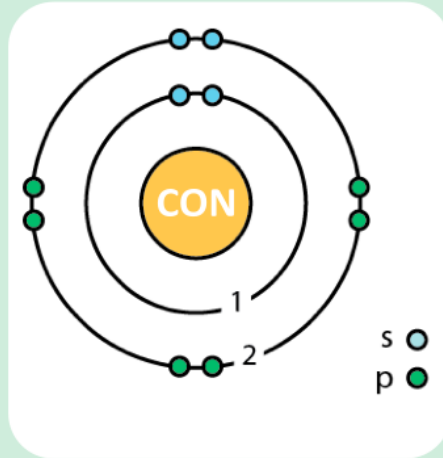


# Doğru Bilgiye Nasıl Ulaşırız?



# 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!**

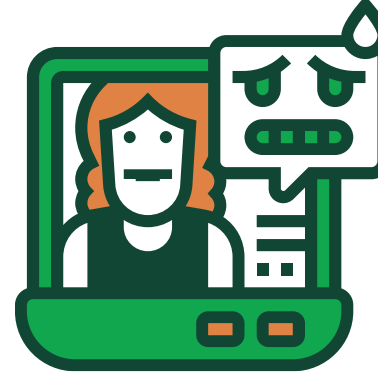
Bugün ABD, AB, bilimum Asya ülkeleri Avustralya, Antartika ve Afrika Contorium elementinin peşinde!



# 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**, sosyal medya, mesajlaşma, oyun gibi dijital platformlarda, kişiyi korkutmayı, kızdırmayı veya utandırmayı amaçlayan, tekrarlanan 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 kurması 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.

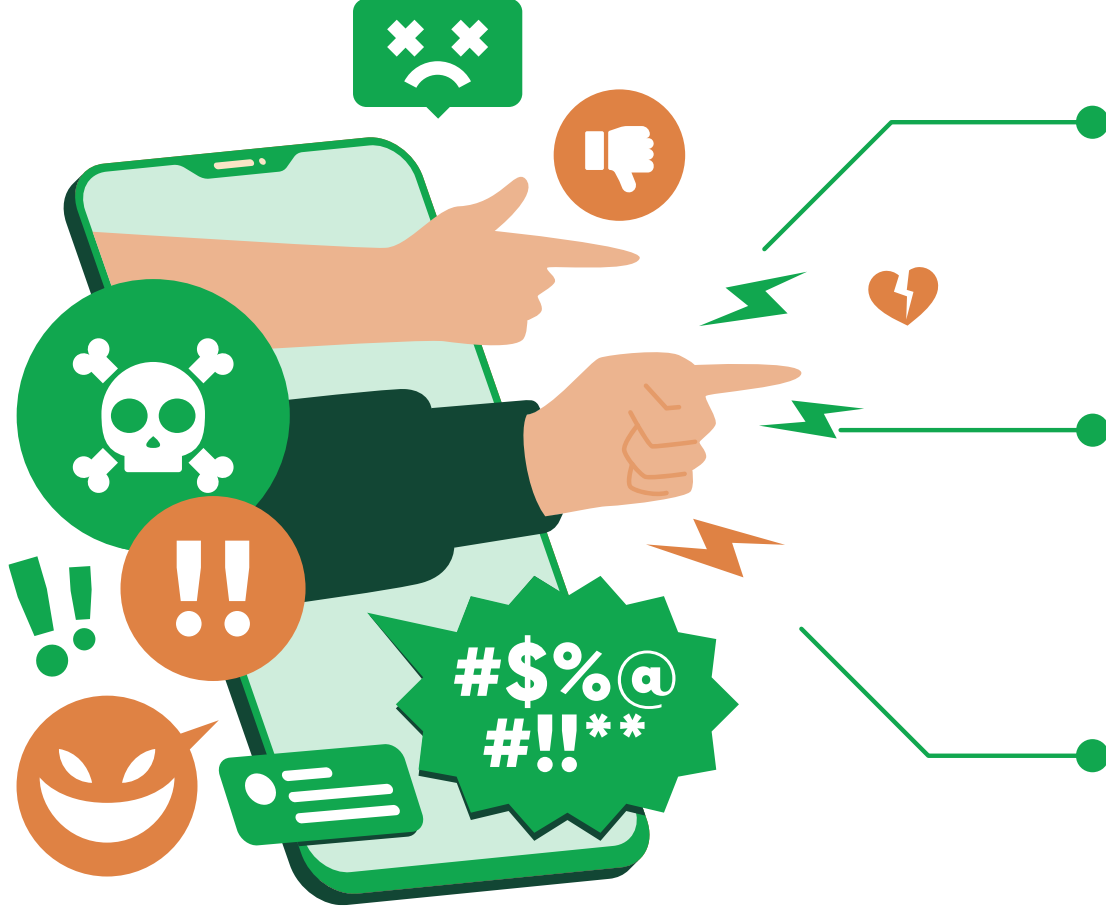
Zorba anonim olabilir.

Zorbaliğa uğrayan kişi ile empati kurmak zordur.

Zaman ve mekandan bağımsızdır.

Zorbaliğa uğrayan kişi kolayca zorbaya dönüşebilir.

# Siber Zorbalık



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 çevrim içi 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?

**Çevrim içiyken sana nasıl davranılmasını istiyorsan sen de insanlara öyle davran.**



# Siber Zorbalık Türleri

**Dışlama:** Kasıtlı olarak belli kişi ya da kişileri çevrim içi 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 çevrim içi 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 çevrim içi ortamda yayınlarak 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

**Trolleme:** Bir kişinin internette kışkırtıcı yorumlar yayınlarak kasıtlı olarak başkalarını üzmeye çalışmasıdır. Trollük her zaman bir siber zorbalık biçimi olmayabilir, ancak kötü niyetli, siber zorbalık için bir araç olarak kullanılabilir. Kişiler arasında çoğunlukla kişisel bir ilişkileri yoktur.

**Israrlı Siber Takip:** Bir kişiyi küçük düşürmek veya gerçek dünyada onunla tanışmak amacıyla çevrim içi aktivitelerini izleme eylemidir.





# Siber Zorbalık Türleri

**Çevrim içi 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 çevrim içi ortamda söylediklerini o kişinin yüzüne söylemesi pek olası değildir (özellikle buna şahit olacak bir arkadaş, ebeveyn veya öğretmen varsa).



# Siber Zorbaliđa Uđramanın Kiřiye Etkileri



## ZİHİNSEL ETKİLER

sevdiđi řeylere karřı  
ilgisini kaybetmesi



## DUYGUSAL ETKİLER

- üzgün
- utanmıř
- sersemlemiř
- kızgın hissetmek



## FİZİKSEL ETKİLER

yorgunluk  
uykusuzluk  
mide ađrısı  
bař ađrısı

# 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 Zorbaliđa Uđrarsam Ne Yapabilirim?

- Zorbaliđa uđradıđını dűşünüyorsan, öncelikle çaresiz olmadığını bil. İlk adım olarak sana yardım edebileceđini dűşündüğün bir yetiřkinden yardım isteyebilirsin.
- Okulunda bulunan psikolojik danıřmana veya sevdiđin bir öğretmene ulařabilirsin.
- Zorbalık sosyal bir platformda gerçekteřiyorsa, zorbayı hemen engellemeyi ve davranıřlarını sosyal medya platformunun kendisine de resmi olarak bildirmeyi ihmal etme.



# Siber Zorbaliđa Uđrarsam Ne Yapabilirim?

- Gerektiđinde kullanmak üzere rahatsız edici ieriklerin görüntülerini alarak kanıt toplayabilirsin. Yasal haklarını 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

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 İin İpuları



İnternette veya sosyal medya hesaplarında kişisel bilgilerini (T.C. kimlik no, telefon, adres, yaşı, 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 İin İpuları



Hesap gizlilik ayarlarını deęiřtirerek kimlerin profilini grebileceęine, sana doęrudan mesaj gnderebileceęine veya gnderilerine yorum yapabileceęine karar verebilirsin.



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

# İnterneti Güvenli Kullanım İin İpuları



Halka aık ya da bilmediėin alanlardaki wifi aėları tehlikeli olabilir. Bu aėlar kişisel bilgilerini almak iin oluşturulmuş sahte bağlantılar olabilir.



Bluetooth veya Airdrop'u kullanmadıėın zaman devre dıőı bırak. Bu bağlantı birçok cihazın birbiri ile etkileşim halinde bulunmasına olanak sağlar ve bir hacker bu aık Bluetooth bağlantıları iinden cihazına erişim sağlayabilir.



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

# İnterneti Güvenli Kullanım İin İpuları



Herhangi bir ierik paylařmadan nce dur ve bu ierik ile biri sana zarar verebilir mi, sen başkasına zarar verir misin diye iyice dřn.



Paylařtıđın fotođrafların / videoların kt niyetli insanlar tarafından deđiřtirilebileceđini unutma. Bu yzden paylařtıđın fotođrafları seerken dikkatli ol.



Artık kullanmadıđın hesaplarını sil veya devre dıřı bırak. Eđer ylece bırakırsan haberin bile olmadan ele geirilebilir.

# İNTERNETİN GÜVENLİ KULLANIMI ve SİBER ZORBALIK

Teşekkür ederiz



TÜRKİYE BAĞIMLILIKLA  
MÜCADELE  
EĞİTİM PROGRAMI

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