



Co-funded by the  
Erasmus+ Programme  
of the European Union

# Yaşamım Dijitalleşiyor Sağlıklı Dijital Yaşam için 10 Strateji

Editörler

Mehmet TABAK - Emre TAMAS



**HD-LIFE**  
**PROJECT**

**İletişim:**

Mehmet TABAK  
Kayseri İl Emniyet Müdürlüğü  
**E-mail:** mehmet.tabak@egm.gov.tr

**Yayın Komisyonu:**

Cavit ÖZBEK  
İlhan DURAN  
Hakan İBİŞOĞLU  
Mehmet TABAK  
Emre TAMAS

Bu entelektüel çıktı “Öğrenciler için Sağlıklı Dijital Yaşam” Projesi kapsamında üretilmiştir. “Öğrenciler için Sağlıklı Dijital Yaşam” Projesi Erasmus+ Programı kapsamında Avrupa Komisyonu tarafından desteklenmektedir. Ancak burada yer alan görüşlerden Avrupa Komisyonu ve Türkiye Ulusal Ajansı sorumlu tutulamaz.

<http://hdlife.erciyes.edu.tr/>



Co-funded by the  
Erasmus+ Programme  
of the European Union



**Tasarım:** Kayseri İl Emniyet Müdürlüğü  
HD-LIFE Projesi, 2019

# Ön Söz

Dijital yeterliliğin kilit bileşenleri Avrupa Komisyonu’nca 5 alanda özetlenmektedir. Bunlardan biri “güvenlik”tir. Güvenlik; dijital ortamlardaki riskleri ve tehditleri anlamayı, güvenlik önlemlerini bilmeyi ve güvenilirliği ve mahremiyeti göz önünde bulundurmaya, dijital teknolojileri kullanırken fiziksel ve psikolojik sağlığa yönelik risklerden ve tehditlerinden kaçınabilmeyi, kendini ve başkalarını, dijital ortamlarda olası tehlikelere karşı koruyabilmeyi ve dijital ortamlarda kişisel verileri ve mahremiyeti korumayı amaçlar. Bilgi ve veri okuryazarlığında ise veri, bilgi ve dijital içeriğin kaynaklarının güvenilirliğini analiz etmek, karşılaştırmak ve eleştirel bir yaklaşımla değerlendirmek, verileri, bilgileri ve dijital içeriği analiz etmek ve eleştirel bir yaklaşımla değerlendirmek yeterlikler arasında sayılır. Elinizdeki bu kitapçık çoğunlukla dengeli ve sağlıklı bir çevrimiçi hayatın tanıtımına sizleri de dâhil ederek dijital sorunların önlenmesini hedefleyen bir eğitim eylemini bildirmektedir. Bu eylemin amacı, sizlere dijital aktivitelerinizde bilinçli-akıllı, sorumlu ve saygılı olmaya yönlendiren bir yol açmak ve onların arkasındaki etik sonuçları anlamana yardımcı olmaktır. İnternet ve mobil iletişim teknolojilerinin endişe kaynağı olabileceği hususlar ve bu sorunları olumlu yönde aşma çabalarına katkı sunmayı amaçlayan bu kitapçığın içeriksel tasarımına önerileriyle katkı sunan HD-LIFE Projesi Koordinatörü Prof. Dr. Hakan AYDIN’a bu vesileyle çok teşekkür ederiz.

# İÇİNDEKİLER

|                                                                   |    |
|-------------------------------------------------------------------|----|
| İnternet Ortamında Doğru ve Güvenilir Bilgiye Nasıl Ulaşabiliriz? | 3  |
| Siber Zorbalıktan Nasıl Korunmalıyız?                             | 4  |
| Siber Güvenliğimizi Nasıl Sağlarız?                               | 9  |
| İnternet Bağımlısı Mıyım?                                         | 16 |
| Dijital Oyun Bağımlılığı                                          | 19 |
| Dijital Mahremiyetimizi Nasıl Koruyabiliriz?                      | 20 |
| İnternet, Fiziksel ve Psikolojik Sağlığımız İçin Bir Tehdit Mi?   | 22 |
| Popüler Bir Dijital Sorun: Cinsel Sömürü ve Mesajlaşma            | 25 |
| Sağlıklı Dijital Yaşam Kontrol Listesi                            | 29 |
| Sağlıklı Dijital Yaşam Sözleşmesi                                 | 30 |



## İnternet Ortamında Doğru ve Güvenilir Bilgiye Nasıl Ulaşabiliriz?

Vazgeçilmezimiz, neredeyse her derdimize deva olduğunu düşündüğümüz, alışverişten yol bulmaya, banka işlemlerinden iletişime, fotoğraflarımızı ve dertlerimizi paylaşmaktan, fikirlerimizi olağanca sertliğiyle ifade etmeye kadar geniş bir yelpazede başvurduğumuz internet acaba ne kadar güvenilir bir bilgi kaynağı?

Hiç düşündünüz mü?

Günümüzde insan yaşamının vazgeçilmez parçalarından biri haline gelen ve internete bağlanabilen bilgisayar ve benzeri gereçler; sıklıkla sohbet, oyun, iletişim, paylaşım gibi kişisel amaçlarla etkin bir biçimde kullanılıyor. İş insanları ve bilimsel çalışmalar yapan araştırmacılar için ise internet önemli bir araç ve kaynak niteliğinde. Hele günümüzde sıklıkla yapıldığı gibi herhangi bir amaçla araştırma yapmak, bilgi toplamak ve bu bilgileri analiz etmek istiyorsak internet, az zamanda çok iş yapabilmenin önemli araçlarından biri. İşte bu noktada, internet kullanarak erişim sağladığımız web sayfalarının ve buralarda karşılaştığımız bilgilerin ne kadar güvenilir olduğu veya güncel olup olmadığı soruları akıllara gelmektedir. Zira, pek çok web sitesinde olduğu gibi bazı içeriklerin kopyala-yapıştır yöntemiyle üretilmesi ve alıntılanan kaynaklara referans verilmemesi, pek çok içerikte yazar bilgisinin yer almaması gibi sorunlar, söz konusu sitelerin ve içeriklerin ne kadar güvenilir olduğuna yönelik kuşkuyla doğmasına sebebiyet vermektedir.

### İşte Bu Noktada Bireysel Kullanıcılar Olarak Bizler Neler Yapmalıyız?

#### 1- Sosyal mecralarda karşılaştığınız haberleri veya içerikleri farklı kaynaklardan teyit edin;

Online mecralarda karşılaştığınız bir haberin veya bilginin doğruluğundan emin olmak için aynı haberi ya da bilgiyi farklı platformlardan araştırın ve orjinal kaynaklardan teyit edin.

#### 2- URL/Adres gerçek mi;

Sahte haber siteleri, güvenilir ve resmi haber kaynaklarına çok benzeyen, taklit edilmiş bir adres, (URL) adresi kullanırlar. İnternet adreslerine dikkat edin.

#### 3- İddialı başlıklara ve reklamlara dikkat edin;

Olağan dışı iddialar, ilgi çekmek için abartılmış başlıklar ve çok fazla kullanılmış noktalama işaretleri, genellikle asılsız haberlere veya reklam içerikli haberlere aittir.

#### 4- Okuduğunuz haberin tarihini kontrol edin;

Haber sitelerinin stratejilerini, haber vermekten ziyade hit kazanmak, “ziyaretçi sayısını arttırmak” üzerine kurguladığını unutmayın. Okuduğunuz haberlerin tarihlerini mutlaka kontrol edin. Gündemle ilgili olabilecek ancak eski tarihli bir haber daha fazla tıklansın diye dolaşıma sokulmuş olabilir. Eski tarihli bir haberi yeniymiş gibi yaygınlaştırmak da internette yanlış bilginin dolaşıma girmesine sebep olur. Bir olayın “daha önceden yaşanmış olması” ve “gerçek olması” onun tarihinin eski olduğu ve başka bir olaya ait olduğu gerçeğini değiştirmeyecektir.

#### 5- Fotoğrafları Google’da aratın;

Google, her gün kullandığımız bu arama motorunu iyi bildiğimizi düşünürüz. Ancak Google’ın çok fazla bilinmeyen bazı özellikleri internette arama yapma ve aradığımızı bulma yeteneğimizi güçlendirebilir. Bunlardan en önemlisi belki de Google Görsel Araması’dır.

Google anasayfasının sağ üst kısmında “Görseller” ifadesi yer alır. Bu linkten Google’da görsel aratabilirsiniz. Arama çubuğundaki fotoğraf makinası ikonuna tıklarsanız, elinizdeki bir görseli de Google’a sorabilirsiniz. Böylece Google, elinizdeki görsele en yakın sonuçları internette arayarak bir fotoğrafın daha önce kullanılıp kullanılmadığına dair size en sağlam bilgiyi vermiş olur. Eğer tarayıcı olarak Google Chrome kullanıyorsanız sosyal medyada gördüğünüz bir fotoğrafa sağ tıklayıp, “Görsellerde ara” seçeneğine tıklayarak, Google’da aratabilirsiniz.

#### **6- Fotoğrağların EXIF bilgisini kontrol edin;**

Her fotoğraf arkasında bir iz bırakır. EXIF ile dijital fotoğrağların arkasında yazan verileri kastediyoruz. Fotoforensics gibi araçlar ile bir fotoğrafın ne zaman, hangi cihazla, hangi açıyla, hangi ışıkla ve -eğer cihaz cep telefonuysa ve kamerası konum servislerini kullanıyorsa Facebook, Twitter’a yüklenen fotoğrağların EXIF bilgisinin bu araçlar tarafından silindiğini unutmayın. Ayrıca EXIF kolayca manüpile edilebilen, değiştirilebilen bir bilgi. Bu yüzden yalnızca EXIF bilgisiyle bir fotoğrafı yüzde 100 doğrulamak imkansız.

### **Siber Zorbalıktan Nasıl Korunmalıyız?**

Son yıllarda sıklıkla duymaya başladığımız “siber zorbalık” kavramı, internetin yaygınlaşmasıyla ortaya çıkan yeni bir zorbalık türüdür. Sosyal ağlar, mesaj grupları, videolar ve dijital oyunlar en çok çocuklar ve gençler için birtakım riskler barındırmaktadır. İnternet kullanım oranlarındaki artış ve kullanım yaşının giderek düşmesiyle beraber, tüm dünyada siber zorbalıkla karşılaşma oranı da giderek artmaktadır.

O halde siber zorbalık nedir? Siber zorbalık en genel tanımıyla çocuklar ya da ergenlerin başka çocuklar ya da ergenler tarafından internet, dijital teknolojiler ya da cep telefonları aracılığıyla eziyet, tehdit, taciz, küçük düşürülme, utandırılma ve benzeri şekillerde hedef alınmasını ifade etmektedir. Başka bir ifadeyle, elektronik iletişim araçları kullanılarak bir kişi ya da gruba yönelik zarar ya da rahatsızlık verici eylemlerde bulunmak şeklinde tanımlanabilmektedir.

#### **Siber Zorbalık Davranışlarının Nedenleri**

- Kullanıcı adlarının arkasına saklanabilme kolaylığı,
- Kimliği bilinmeyen daha güçlü olduğuna yönelik içgüdüsel hissiyat,
- Bilinmeden ortamı etkilemenin çekiciliği,
- Zorbaların verdikleri zararların sonuçlarını görememeleri,
- Popüler olma isteği,
- Yaşadıklarını farklı yansıtmaya eğilimi,
- Düşük özgüven ve daha önce siber zorbalığa maruz kalma,
- Sosyal kaygı,
- Aile içi huzursuzluklar vb.

**Peki, hangi eylemler siber zorbalık kapsamına girer;**

**Dedikodu:** Kamuoyunda spekülasyon oluşturma. Çevrimiçi ortamlarda hakkınızda kasıtlı ve alenen dedikodu yapılması.

**Dışlama:** Bir grup arkadaştan bir kişiyi ayırma. Özellikle okulda başlayan ve siber ortamda devam eden dışlanma.

**Taciz:** Sürekli ve kasıtlı olarak yapılan zarar verici ve rahatsız edici davranışlar.

**Takip:** Her an izlenildiğini hissetme. İnternette başlayıp, gerçek hayata yansıyan takip ediliyormuş hissi.

**Trollemek:** Kasten ve maksatlı olarak yapılan provokasyon (kışkırtma) ve örtülü hakaret.

**Yorumlar:** Yazı, fotoğraf, video yoluyla yapılan hakaret ve küfür içeren negatif iletiler.

**Saygısızlık:** İletişimde haddi aşmak ve bunu devam ettirmek.

**Sahte Hesap:** Kurban adına sahte hesaplar oluşturularak ve bu oluşturulan sahte hesaplar yoluyla tehdit ve zorbalığı sürdürmek.

**Kandırma:** Başkalarının çeşitli, gizli bilgilerini yayınlayarak ve bunları çarpıtarak insanları aldatmak, dolandırmak.

**Manipüle:** Kurbanın kendisi gibi davranmak.

Yukarıda sıralanan durumlara maruz kalmışsanız siber zorbalıkla karşı karşıyasınız demektir.





### Siber Zorbalıklarla Nerelerde Karşılaşıyoruz?

- Sosyal paylaşım siteleri (Facebook, Twitter, Instagram vb.)
- Online oyunlar
- E-posta
- Fotoğraf ve video paylaşımı
- Sohbet odaları
- Telefon mesajları
- Telefon görüşmeleri

### O Zaman Birey Olarak Siber Zorbalıktan Nasıl Korunmalıyız?

- Her şeyden önce iletişim araçları ve internet bilinçli kullanılmalıdır.
- Ele geçirilmesi ve tahmin edilmesi zor kullanıcı şifresi belirlenmelidir.
- Güvenlik (antivirüs vb.) yazılımları güncel olmalıdır.
- Yüz yüze ilişkilerdeki etik kurallar sanal ortamda da aynıyla uygulanmalıdır.
- Tanımadığınız kişilerden gelen mesajları okumamak, onaylamamak, paylaşmamak ve engellemek sizi her zaman daha güvenli kılar.
- Kişisel bilgileriniz size özeldir, başkalarıyla paylaşılmamalıdır.
- Web sitelerini gezinirken şüpheli olun, bilginin kaynağını araştırın ve kişisel bilgilerinizi her web sitesinde paylaşmayın.
- Size gelen kimliği bilinmeyen maillere dikkat edin. Sahte hesap olma ihtimalini göz önünde bulundurun ve bu gibi durumlarda dikkatli olun.

- Gerçek hayattaki davranış biçimi sanal ortamda da korunmalı ve siber zorbalığın suç olduğu bilinmelidir.

### **Siber Zorbalıktan Korunmak İçin Ebeveynler ve Aileler Neler Yapmalılar?**

- Bilgisayar, cep telefonu ve diğer teknolojik araçlar için uygun kullanma kuralları belirleyin. Örneğin çocuklarınıza, hangi siteleri ziyaret edebileceklerini, hangilerini onaylamadığınızı, açıkça belirtin.
- İnternet kullanımına ilişkin onaylamadığınız davranışları nedenleri ile birlikte açıklayın.
- Kuralların kolayca benimsenmesi için çocuğunuzun bu kurallara ilişkin itirazlarını ve onun nedenlerini de dinleyin. Bu kuralların belirlenmesine çocuklarınızı dahil etmek, bu kuralların benimsenmesini sağlamak adına önemlidir.
- Çocuklarınızın paylaşımlarını akıllıca yapmaları konusunda onlara yardımcı olun. Kendilerine ya da başkalarına zarar verebilecek paylaşımlardan kaçınmalarını söyleyin.
- Çocuklarınızı, paylaştıkları içeriğin kimler tarafından görüleceği konusunda yönlendirin. Tanımadıkları kişilerle sosyal ağlarda da olsa iletişime girmenin riskleri konusunda konuşun.
- Çocuklarınıza, şifrelerini kimseyle paylaşmamalarını söyleyin. Çünkü şifre paylaşmak onların kimlikleri ve aktiviteleri üzerindeki kontrollerinden ödün vermelerine neden olur. Siber zorbalık vakalarının bir kısmı, şifrelerin arkadaşlarla paylaşılmasından kaynaklanmaktadır.
- Okul sınırları içinde teknoloji kullanımıyla ilgili kuralların konulması ve uygulanması konusunda okul yönetimi ve öğretmenlerle işbirliği içinde olun. Kendilerine ya da başkalarına zarar verebilecek paylaşımlardan kaçınmalarını söyleyin.
- Çocuklarınızı, paylaştıkları içeriğin kimler tarafından görüleceği konusunda yönlendirin. Tanımadıkları kişilerle sosyal ağlarda da olsa iletişime girmenin riskleri konusunda konuşun.



## SİBER ZORBALIKLA MÜCADELEDE 10 KRİTİK ADIM



### 1. AİLENLE PAYLAŞ

Bilgisayarım, akıllı telefonum ya da diğer elektronik cihazlarım aracılığıyla beni rahatsız eden bir kişi veya durum olursa derhal bunu ailemle paylaşacağım.



### 2. AİLENDEN İZİN AL

Aile büyüklerimden izin almadan kendime veya başkalarına ait hiçbir fotoğrafı, videoyu ve görsel materyali sosyal ağlarda ya da diğer online platformlarda paylaşmayacağım.



### 3. İZİNLİ İLETİŞİM KUR

Anne ve babamın haberi ve izni olmaksızın, tanımadığım kişilerle online olarak görüşmeyeceğim. Böyle kişilerle akıllı telefon aracılığıyla iletişim kurmayacağım.



### 4. KÖTÜ MESAJLARI BİLDİR

Beni tehdit veya rahatsız eden, dalga geçen ya da kendimi kötü hissetmeme neden olan her türlü mesajı önce anne ve babama bildireceğim. Bu tür mesajları almamın kesinlikle benim suçum olmadığının farkında olacağım.



### 5. KİMSEYİ İNCİTME

Kendim de bir siber zorba olmayacağım! Sosyal medya, e-posta veya akıllı telefon gibi dijital iletişim araçlarını kullanarak kimseyi incitecek söz yazmayacak, dedikodu yapmayacağım.



### 6. KİŞİSEL BİLGİLERİNİ PAYLAŞMA

Ev adresimizi, telefon numaramı, aileme ait iş yeri ve telefon bilgilerini onların haberi ve izni olmadan kesinlikle hiç kimseyle paylaşmayacağım.



### 7. ŞİFREİNİ PAYLAŞMA

Bilgisayarımda, sosyal medyada ve mobil cihazlarımda kullandığım şifreleri ailem dışında kimseye söylemeyeceğim. Bu şifreleri isteyen bir arkadaşım bile olsa, hemen anneme veya babama haber vereceğim.



### 8. İÇERİĞİ AİLENLE BELİRLE

İnterneti ve sosyal medyayı kullanacağım zamanı, ziyaret edebileceğim web sitelerini ve uygulamaları aile büyüklerimle birlikte belirleyeceğiz.



### 9. İNTERNETİ DOĞRU KULLAN

Ailemin tüm bireylerinin interneti doğru şekilde kullanmasını, daha keyifli vakit geçirmelerini ve yeni şeyler öğrenmelerini sağlamak için onlara yardımcı olacağım.



### 10. DOSYALARI İZİNLE İNDİR

Bilgisayarıma, akıllı telefonuma ya da diğer elektronik cihazlarıma herhangi bir dosya, uygulama veya görüntü indirmeden önce mutlaka anne ve babamın iznini alacağım.

## Siber Güvenliğimizi Nasıl Sağlarız?



#### ✓ Zararlı Yazılımlar (Malware):

En genel ifade ile bilgisayar sistemlerini kötü amaçlı kullanmak için sistem bilgilerine erişim sağlamaya yarayan ya da bilgisayar sistemlerine ciddi zararlar veren kötücül bilgisayar programlarıdır. Zararlı yazılımlar genel bir kavram olup virüsler, solucanlar, truva atları, rootkitler ve casus yazılımlar bu konseptin içerisinde kendine yer bulabilirler.



#### ✓ Virüsler:

Bilgisayar virüsleri en genel manada kendini sistemdeki dosyalardan ya da programlardan biri olarak değiştiren bilgisayar kodlarıdır. Virüslerin anlaşılmasındaki kritik nokta ise bir kullanıcı tarafından çalıştırılmaları gerektiridir. Genellikle bir kullanıcıdan gelen e-postanın açılması, ya da USB'nin otomatik çalıştırılması şeklinde meydana gelebilmektedir.



#### ✓ Solucanlar:

Virüs gibi kendini bir bilgisayardan başka bilgisayara kopyalamak için tasarlanmış zararlı yazılımlardır. Virüslerden farkı, yayılma işlemini ağ üzerinden otomatik olarak yapmasıdır. Otomatik yayılmanın olması nedeni ile zamanla bilgisayar ağının yavaş çalışmasına, internet sayfalarının geç gelmesine neden olurlar.

#### ✓ Yemleme (Phishing):

Yasadışı yollarla kullanıcıların herhangi bir sistem için kullandıkları kullanıcı adı, şifre, kimlik bilgileri, kredi kartı ayrıntıları gibi bilgilerin ele geçirilmesidir. Sözcük, İngilizce password (şifre) ve fishing (balık avlamak) sözcüklerinin birleşmesiyle oluşturulmuş “phishing” ifadesinin Türkçe karşılığıdır. “Yemleyici” diye tanımlanan şifre avcıları, genelde e-posta gibi yollarla kişilere ulaşır ve onların kredi kartı gibi ayrıntılarını sanki resmi bir kurummuş gibi ister. Bu tip mailleri cevaplayan kullanıcıların da hesapları, şifreleri vb. özel bilgileri çalınmaktadır.



### ✓ Sosyal Mühendislik:

Temel olarak bilgisayar ya da bilgisayar ağlarındaki açıklıklardan faydalanarak bilgisayar sistemlerine zarar veren yaklaşımların aksine “sosyal mühendislik” yöntemi; insanların iletişim, düşünce tarzı, güven ya da kısaca insani zaaflarından faydalanarak siber güvenlik süreçlerinin etkisiz hale getirilmesi ya da atlatılması şeklinde tanımlanabilir. Sosyal mühendislik yöntemleri; çeşitli yalanlar yolu ile sahte senaryolar üretmek, hedef kişiye kendini güvenilir bir kaynak olarak tanıtmak ya da basit ödüllendirme yöntemleri ile bilgi sızdırmak şeklinde özetlenebilir.



### O Halde, Birey Olarak Siber Güvenliğimiz İçin Neler yapmalıyız?

#### ✓ Anti-virüs Yazılımı Çalıştırın,

Çoğu bilgisayar anti-virüs yazılımı ile birlikte gelir ve çalışanların, bilgisayarlarını düzenli olarak kontrol etmeleri gerekir. Yazılımlar, en güncel koruma tehdidini (virüs) tespit eder ve bir virüsün sistem üzerinde çoğalma aşamasını engelleyerek sabit sürücünden kaldırır.

#### ✓ Verileri Yedekleyin,

Tüm teknolojiler gibi, bilgisayarlar da dört dörtlük değildir ve en olmadık zamanlarda çökebileceği bilinmektedir. Çalışmalarını ve işlemlerinin çoğunu bilgisayar üzerinde gerçekleştiren kişilerin düzenli aralıklarla verilerini yedeklemesi çok önemlidir. Eğer bilgisayar arızalanır ve bilgiler başka bir yerde depolanmazsa, bu verileri kurtarmak mümkün



olmayabilir. Yıllar ya da aylar alan yoğun bir çalışmanın korunması için değerli iş belgelerini, e-postaları ve verileri yedekleyebileceğiniz taşınabilir sabit sürücüye yatırım yapabilirsiniz.

#### ✓ Bir Güvenlik Duvarı Edinin,

Güvenlik duvarı; erişilen bilgisayarlardan gelen, onaylanmayan internet trafiğini önleyen yazılımlardır. Bu uygulama düzgün bir şekilde yapılandırıldığında, insanlara kendi cihazlarını daha fazla kontrol edebilme imkanı sağlar ve bilgisayar ağına yönelik saldırılar önlenabilir.

#### ✓ Orijinal Parolalar Oluşturun,

Özgün parolalar, bilgisayarların istenmeyen kişilere karşı erişilebilir olmasının önüne geçecektir. Bir hacker ya da bir hırsız, bilgisayara erişmek için girişimde bulunursa, giriş yapabilmek için doğru parolayı girmeye ihtiyacı olacaktır. Parolalar, tahmin edilmesi kolay olan şeyler olursa, genellikle hackerlar bu kodu kırabilirler. Meydana gelen bu basit ihlali önlemek için yaratıcı olun ve parolanızda en az üç tip farklı karakter kullanın.

#### ✓ Bilinmeyen E-postaları Engelleyin,

Çoğu virüs, bilgisayarlara e-posta eklentileri ( .vbs, .scr, .exe ve . pif uzantılı eklentiler) aracılığıyla bulaşmaktadır. Bir çalışan, bilinen ya da bilinmeyen göndericilerden, bu uzantıları barındıran herhangi bir ek ile birlikte e-posta alırsa, bu dosyalar yüzünden bilgisayarın etkilenmeyeceğinden emin olmak için antivirüs yazılımını çalıştırabilir veya güvenmeyen yerlerden gelen mailler açmadan silebilir.

#### ✓ Siber Güvenlik İçin Ebeveynlere Düşen Görevler;

- Bilgisayarınızın işletim sistemini güncel tutun.
- Bilgisayarınıza mutlaka güvenlik duvarı içeren bir anti-virüs programı yükleyin. Anti-virüs programınızı düzenli olarak güncelleyin.
- Sosyal ağlarda ve web tarayıcılarınızda gizlilik ve güvenliğe dikkat edin. Sosyal ağlarda profilinizi arama motorlarına, tanımadığınız kişilere ve 3'ncü şahıslara reklam amaçlı verilmesi girişimlerine karşı kapalı tutun.
- Kişisel bilgilerinizi ve ileride pişman olacağınız içerikleri internette, özellikle sosyal ağlarda paylaşmayın. Çünkü internette her bilgi silinmeden kalabilir.
- Özellikle çocukların akıllı telefonları kullandığı düşünülürse, “Güvenli İnternet Çocuk Profili” muhakkak aktif hale getirilmelidir.



## Prensesler Unutmayın!

İnternet bir masal dünyası gibi büyü... Masalarda cadılar varsa, internette de kötü insanlar var.

Siz internette her zaman iyi bir kullanıcı olmaya çalışın, yasal olmayan ve başkalarına zarar verebilecek davranış ve paylaşımlar yapmaktan kaçının!

SİBER SUÇLARLA MÜCADELE  
DAİRE BAŞKANLIĞI

[www.siber.pol.tr](http://www.siber.pol.tr)  
[siber@egm.gov.tr](mailto:siber@egm.gov.tr)

**SİBER POLİS** sizin güvenliğinizi için çalışıyor siz de önerilerimizi uygulayarak güvenliğinizi sağlayabilirsiniz



Kötü ve sizi rahatsız eden mesajlara hiçbir zaman cevap vermeyin. Böyle bir mesaj almanız sizin suçunuz değildir. Böyle bir mesaj alırsanız anne ve babanıza veya güvendiğiniz bir yetişkine söyleyin. Onlar da bunu **Siber Polis**'e bildirsinler.





En sevdiğiniz web siteleri ve uygulamaların nasıl çalıştığını ailenize gösterin. Onların internette neler yapılabileceğini anlamalarına yardımcı olun. Twitter ve Facebook gibi sosyal ağların kullanım kurallarına uyun.



Ev adresinizi, telefon numaranızı ve okulunuzun ismi ve yeri gibi kişisel bilgilerinizi internette paylaşmayın. Anne ve babanızın kişisel bilgilerini de internette kullanmayın.



Resimlerinizi kime gönderdiğinizize dikkat edin. Bazı kişiler bu resimleri sizlere zarar vermek için kullanabilirler.



Tanımadığınız veya güvenmediğiniz kişilerden gelen mesajlardaki ekleri açmayın; Bu mesajlar virus içerebilir. Bu virüsler kişisel bilgilerinizin çalınmasına neden olur.



Program yüklerken anne babanıza veya öğretmeni-  
nize sorun. Bazı programlar bilgisayarınıza veya aile-  
nize zarar verebilir. Internette her zaman dürüst olun.





## EN ÇOK UYGULANAN E-HİRSIZLIK YÖNTEMLERİ

### 1 BASİT PAROLALAR

Parolanızı kırmak isteyen hackerlar, öncelikle herkesin kullandığı parolaları dener. "şifre", isminiz, "1234" gibi tahmin edilmesi çok kolay olan parolalar sıkça kullanılıyor.



### 2 SOSYAL AĞ YÖNTEMLERİ

Eğer birinci yöntem işe yaramadıysa bu sefer de size sosyal ağ web sayfanızdan gelmiş gibi parolanızı girmeniz gerektiğini söyleyen sahte bir e-posta gönderebilir ve şifrenizi girmeniz istenebilir.



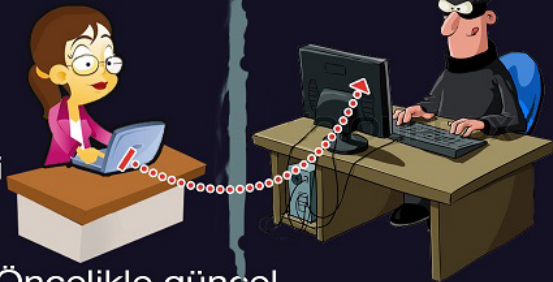
### 3 ŞİFRESİZ Wİ-Fİ AĞLAR

Şifresiz açık Wi-Fi ağları büyük bir güvenlik riski oluşturabilir. Bu ağlardan gönderilen veriler, Wİ-Fİ sinyalinin alınabildiği her yerden izlenebilir. Buna SSL üzerinden gönderilemeyen parolalar da dahildir.



### 4 VİRÜS ve PROGRAMLAR

Zararlı programlar ile bilgisayarınızdaki tüm işlemler ve girilen şifreler hırsızlar tarafından izlenebilir. Bilgisayarınızın ikinci bir sahibi gibi bilgisayarınızı istedikleri gibi kullanabilirler tüm şifre ve hesaplarınızı ele geçirebilirler. Öncelikle güncel antivirüs kullanın güvenli şifre seçin ve asla tanımadığınız kişilerden gelen şüpheli e-postaları açmayın.







# E-GÜVENLİK

SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI  
www.siber.pol.tr

## SANAL KLAVYE KULLANIMI



PC'nize keylogger\* bulaşmış olsa bile sanal klavye kullanımı hesabınızın ele geçirilmesi riskini azaltır.

## E-POSTALARA DİKKAT



Bazı casus yazılım veya virüsler e-posta yoluyla bilgisayarınıza bulaşabilir. Bundan dolayı **tanımadığınız kişilerden gelen veya şüpheli görünen e-postaları açmayın.**

Bilgisayarınıza bir e-mail yada internetten indirdiğiniz film, müzik ve çoğu ücretsiz programların içinde olan bir virüs, gizlenmiş olarak siz farkında olmadan bilgisayar, tablet ve mobil telefonunuza yüklenir. Kişisel bilgi ve şifreleriniz çalınmış olur.

## HIRSIZLARA FIRSAT VERMEYİN !!!

Dünya genelindeki sanal hırsızlar sürekli yeni yöntemler geliştirirken birbirleri ile iletişim halindedirler. Dolayısı ile hırsızlarda sürekli yöntemler geliştirseler de yöntem temelde aynıdır.



**\*Keylogger:** Klavye dinleme sistemi. Klavyenizi kullanarak yazdıklarınızı kaydettikten sonra bunu internet aracılığıyla kötü niyetli kişilere gönderen yazılım.

### Hesap Aktarımı :

Şifrenizin ele geçirilmesi sonrasında arka planda siz farkında olmadan bilgisayarınızdan banka hesabınıza girilir hesabınızdaki paralar hırsızların başka bankalarda bulunan hesaplarına aktarılır.

## İnternet Bağımlısı Mıyım?

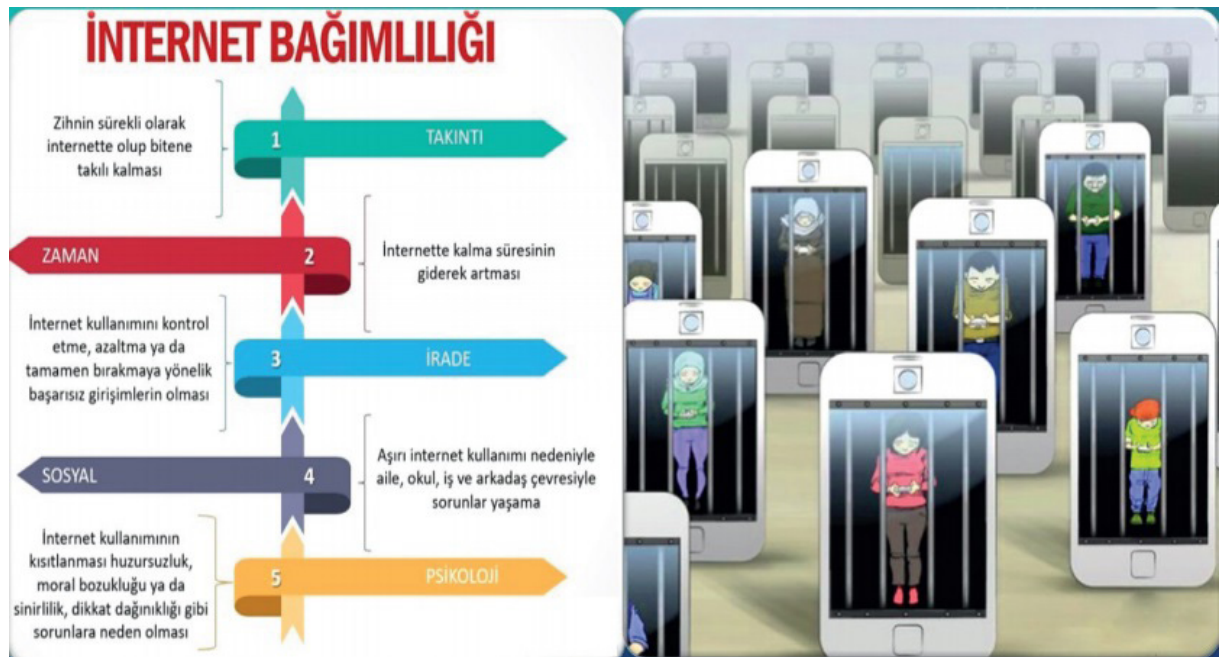


Kullanım alanının her geçen gün artarak genişlemesi interneti vazgeçilmez bir unsur kılarken bu durum birtakım olumsuzlukları da beraberinde getirmektedir. Bilinçli kullanıldığında sayısız avantaj sağlayan internet, diğer yönüyle de bağımlılık riskini ve bağımlılıkla birlikte gelebilecek tehlikeleri ve alışkanlıkları bünyesinde taşımaktadır.

Bağımlılık kişinin kullandığı bir nesne veya yaptığı bir eylem üzerinde kontrolünü kaybetmesi ve onsu bir yaşam sürememeye başlaması olarak tanımlanmaktadır. Son yıllarda internetin, bilgisayarlardan ziyade günün her anı yanımızda bulunan mobil telefonlar aracılığıyla daha fazla kullanılmaya başlanması da bağımlılığı tetikleyen unsurlardan biri olarak göze çarpmaktadır.

İnterneti, insana bu kadar yakınlaştıran cihazlar, internetten gelebilecek riskleri de aynı oranda insana yaklaştırmış oluyor. Tüketim ve alışveriş alışkanlıkları, artan sosyal medya kullanımı, sosyal medya üzerinden pazarlama stratejileri sonucunda bağımlılığa biraz daha yaklaşmak kaçınılmaz olmaktadır.

İnternetin özgür, gizemli ve kolay erişilebilir dünyası özellikle genç nesli gerçek hayattan izole edip yalnızlaştırırken, vaktin kontrolsüzce geçirilmesine de sebep olmaktadır. Duygu ve düşünceleri ifade etmenin en kolay yolu olarak kabul edilmesi, gerçek hayatta kurulamayan ilişkilerin daha rahat kurulabilmesine imkân sağlaması, eğlenmek ve sosyalleşmek gibi sebeplerle internete mecbur kalma gibi faktörler, insanları günümüzün kitle iletişim mecralarından sosyal medya araçlarına bağımlı kılmaktadır.





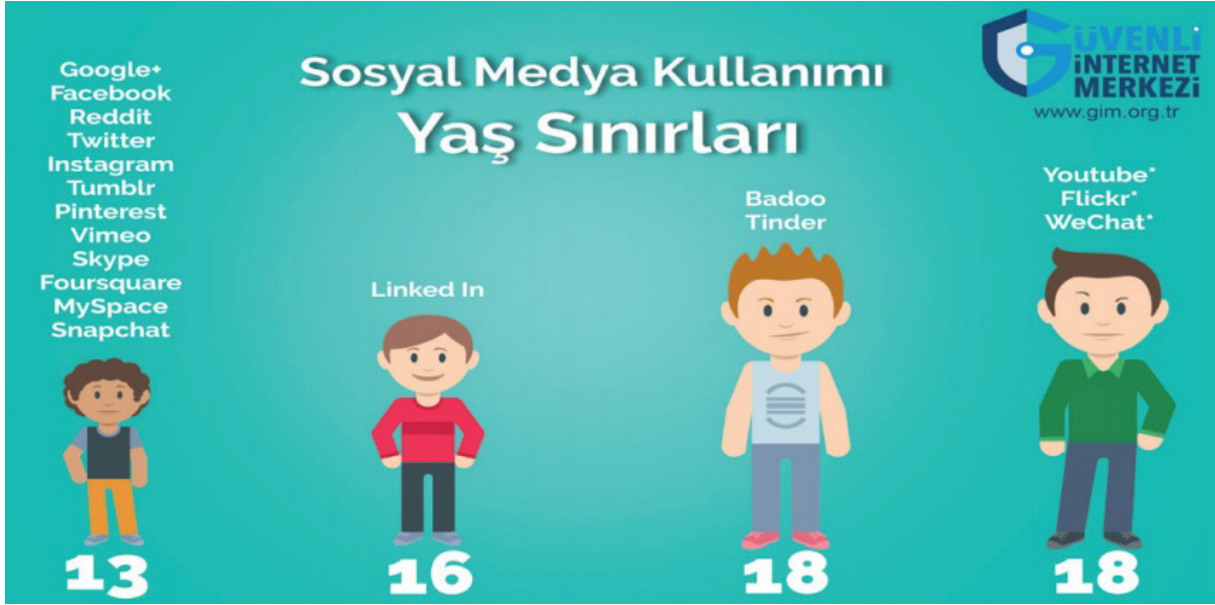
### İnternet Bağımlılığında Ortaya Çıkan Davranışlar:

- Daha az dışarıya çıkmak,
- İnternet kullanımı haricindeki aktivitelere daha az zaman ayırma,
- Ev ya da iş ortamında yemek yemeye daha az zaman harcama,
- İnterneti her defasında daha fazla kullanmayı isteme,
- Genellikle bilgisayar başında yemek yeme alışkanlığı kazanma,
- İnternetin başında geçirilen zamanı kontrol etmekte güçlük çekme,
- Sürekli uykusuz ve yorgun görünme,
- İnternetin başında planlanan süreden daha çok kalma,
- Çevreyle ilişkinin zayıflaması ya da kopması,
- İnternet başında harcanan uzun zamanı inkâr etme,
- Bireyin durumundan başkalarının şikâyet eder olması,
- İnterneti kullandığında kendini daha iyi ve mutlu hissetme,
- Yapılması gereken görev ve sorumluluklar olduğu hâlde internet başından ayrılamama,
- Aile üyeleri evde yokken bunu bir rahatlama ve kurtuluş görüp internete girme,
- İnterneti “iyi hissedilen” tek yer olarak görme.



### Bağımlılıktan Korunmak İçin Öneriler:

- İnternet kullanım süresini yavaş yavaş ama kararlı olarak azaltın,
- İnternetin yerini doldurun, kullanımı azalttığınızda yeni faaliyetlere yönelin (Spor, hobi, vb.),
- Düşünün! Sanal ortamdaki başarı ve saygınlık mı daha değerli, gerçek hayattaki mi?
- Zararlarını, sizden aldıklarını düşünün,
- Gerekirse uzman yardımı alın.



### Teknoloji ile İlişkiniz Nasıl Olmalı?

- Spora ve hobilere vakit ayırın.
- Bilgisayarınızla sırdaş olmayın.
- Ailenizle daha fazla vakit geçirin.
- Mutlaka zaman sınırlaması koyun.
- Kitap okumaya kesinlikle vakit ayırın.
- Öğrenmeye ve ödevlerinize vakit ayırın.
- Dışarıda oyuna ve dinlenmeye vakit ayırın.
- Doğayla vakit geçirmenin rahatlatıcı etkilerinden yararlanın.
- Telefon yanınızda olmadan da dışarı çıkabileceğinizi unutmayın.

### Aşırı İnternet Kullanımında Ebeveynlere Düşen Görevler;

- Kendinizi eğitin, interneti ve sosyal medyayı öğrenin.
- Zaman sınırlaması yapın.
- İnternet kullanımıyla ilgili kurallar belirleyin ve bunu yazılı bir anlaşma şekline getirerek çocuklarınızla altına imzanızı atın.
- Çocuğunuzu uygun bir şekilde uyarın.
- Çocuğunuzla bağlantıyı koparmayın.
- Çocuğunuzun dolaştığı mecraları bilmeye çalışın.
- Sosyal medyada da zararlı içerikli oyunlarla karşılaşma ihtimali yüksek olduğundan, oynadığı oyunlara dikkat edin.
- Çocuğunuza aşırı tepkiler vermeyin.
- Her şeye inanmaması konusunda uyarın.
- Kişisel ve ailevi bilgileri paylaşmamasını öğütleyin.

## Dijital Oyun Bağımlılığı



### Şiddet İçeren Dijital Oyunlara Dikkat!

Son zamanlarda video oyunları ile ilgili yapılan içerik analizleri, oyunların %89'unun şiddet içerdiğini göstermektedir. Şiddet içerikli oyunlar, gelişim aşamasındaki kişiliğe zarar verirken, doğru ile yanlış ayırt edemeyen çocuk ve gençler için oldukça tehlikeli durumlar oluşturabilmektedir. Bazı bilgisayar oyunları ile gençler, oyun üreticisinin bilinçli tercihi ile ruh sağlıkları bozulmak suretiyle, intihara yönlendirilebilmektedir. Örneğin bazı oyunlarda, gece uyanmaları istenen gençlerin hayatı düzensizleştirilmekte, gençler, korku dolu ve gerçeklikle bağı olmayan içeriklere maruz bırakılmaktadır. Günlerce devam eden bu süreçte, gençlere yanlış değer yargıları aşılanmakta ve bu gençler değersizlik hissine itilmektedir. Oyun kılıfı altında kişisel bilgileri "Phishing-Ölüm" yöntemiyle çalınan gençler; tehdit, şantaj ve siber zorbalık yoluyla tuzağa düşürülerek intihara sürüklenebilmektedir.

### Yapılan Araştırmalar Şiddet İçeren Dijital Oyunların,

- Olumlu sosyal davranışlarda azalma
- Düşük yaşam doyumu
- Düşmanca duygularda artış
- Şiddete karşı duyarsızlaşma
- Dikkat sorunları
- Depresyon
- Saldırganlık
- Anksiyete
- Şiddet eğilimi
- Yalnızlık



gibi psikososyal problemlerle ilişkili olduğunu göstermiştir. Şiddet içerikli dijital oyunların psikososyal ve davranışsal problemler ile ilişkisini görmek açısından yapılan bir çalışma



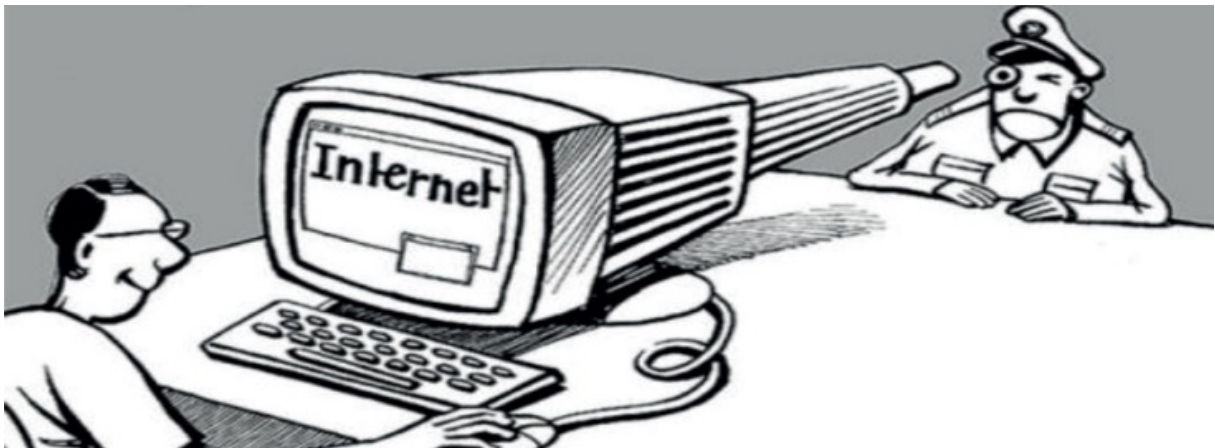
oldukça yol göstericidir. Singapur’lu 3034 çocuk ve ergenin iki yıl izlendiği çalışmada, dijital oyun bağımlılığı - depresyon ve okul başarısı arasındaki ilişki incelenmiştir. Normal oyuncu iken bağımlı hale gelenlerde depresyon, anksiyete, sosyal fobi gelişmiş ve okul performansı kötüleşmiştir. Bağımlı oyuncu iken normal oyuncuya dönenlerde ise depresyon, anksiyete, sosyal fobi ve okul başarısında olumlu yönde gelişme ve düzelmeler görülmüştür.

### Dijital Oyun Bağımlılığına Karşı Birey Olarak Neler Yapabiliriz ?

- Çocuklar dijital oyunlardan uzak tutulamıyorsa, hangi tür oyunları ne kadar ve günün hangi saatinde oynayabilecekleri konusunda kesinlikle kurallar konulmalıdır. Aileler bu kuralları uygulama noktasında kararlı olmalıdır.
- Oyunların içeriği bilinmeli, şiddet içerikli oyunlar oynatılmamalıdır. Gerekğinde çocukların internete girdiği sürede uzaktan erişimle kontrol sağlanmalıdır. Yaşlarına uygun, eğlendirirken eğiten oyunlar seçmeleri konusunda çocuklar yönlendirilmelidir.
- Oyunun içeriği uygun olsa bile süre ve hangi saatte oynayacağı konusunda sınır konulmalıdır. Oyunların içeriği konusunda çocukla konuşulmalı gerçek-sanal ilişkisi anlatılmalıdır.
- Oyun aile bireylerinin olduğu odada kontrol altında oynatılmalıdır. Yalnız çocukların oynaması engellenmeli, aile bireylerinin ortaklaşa oynayabileceği oyunlar tercih edilmelidir. Bunun için masa üstü bilgisayarlar yatak odalarına konulmamalıdır.

### Dijital Mahremiyetimizi Nasıl Koruyabiliriz?

Genel anlamıyla başkalarından sakındığımız, onların görmesini istemediğimiz, kendimize sakladığımız özel konular, kişiler, mekanlar, bilgiler vb mahremiyeti tanımlamak için kullanılır. Bireyler gerçek hayatta olduğu gibi internette de özel yaşamı ve aile yaşamını sürdürme hakkına sahiptirler. Bunun gerçek hayattan ayrı düşünülmemesi gerekir. Çünkü mahremiyetin ihlali ve kişisel verilerin izinsiz kullanımı sadece gerçek hayata ilişkin bir durum olmaktan çıkmıştır. Artık bireylerin, gerçek hayattaki gibi internette de bir kimlikleri, bir mahremiyetleri yani özel hayatları ve kişisel bilgileri mevcuttur. Dolayısıyla bireylerin kişisel verilerinin korunması, yazışmalarının ve iletişimlerinin gizliliğinin sağlanması da bu kapsamda değerlendirilmesi gereken önemli bir husustur.



Mahremiyet bilincine sahipsek internet üzerinde de kontrol sahibiyiz demektir. Herkesin kendine ait özel alanı ve başkalarıyla paylaşmak istemediği şeyler vardır. Mahremiyet bilincine sahip olmak ve mahremiyetimizi koruyabilmek, kendimizi daha güvenli ve özgür hissetmemizi sağlar.

## **Peki Dijital Mahremiyetimizi Nasıl Koruyacağız?**

### **✓ Web Tarayıcısı**

Birinci alan, internet kullanırken web tarayıcımız aracılığıyla veri sızmasının engellenmesi. Çünkü hangi siteyi ziyaret ettiğimiz, neyi aradığımız, hangi parolaları kullandığımız, e-bankacılık işlemleri, e-devlet işleri ve daha fazlası web tarayıcılar tarafından işleniyor. Doğal olarak en fazla kişisel bilgiyi burada kullanıyoruz. Bu yüzden mahremiyet sağlanırken web tarayıcıdan başlanması gerekir. İnternete bağlanmak için birçok tarayıcı var. Bunlardan bazıları işletim sistemi ile birlikte geliyor, bazıları da sonradan yüklenebiliyor. Web tarayıcı eklentilerine baktığımızda kişisel veri sızıntısını önleyen bazı seçenekler olduğunu görüyoruz. Bunlar bağlantıları gözlemleme ve kontrol etme, çerezleri(cookies) engelleme, bir siteden ayrıldıktan sonra tutulacak bilgileri sınırlama, zararlı betikleri (Script), reklamları engelleme olarak sıralanabilir.

### **✓ Mesaj Servisleri Güvenliği**

İnternet üzerinden mesajlaşma her geçen gün artıyor. Hatta Whatsapp, Messenger, Skype gibi araçlar günlük hayatımızın vazgeçilmez bir parçası durumunda. Bu yüzden bu mesajların mahremiyetinin korunması da çok önemli. Çünkü bu mesajların tamamı kişisel ve mahrem bilgiler. Yaygın kullanılan Whatsapp, Telegram, Pidgin, iMessage gibi programlar verileri uçtan uça şifreleyerek veri güvenliğini sağlarlar. Fakat bu bilgiler cihazlarda tutulurken şifresiz tutulur ve bunlara erişimi kontrol altına almak istiyorsanız uygulamaya güvenlik kilidi konulması gerekir.

### **✓ Mobil Mahremiyet**

Mobil cihazlar ve üzerinde çalışan uygulamalar kişisel verileri saklarlar. Telefon çağrıları, metin mesajı bilgileri, fotoğraflar, web gezinme geçmişi, konum bilgileri gibi önemli bilgiler saklanan verilerden yalnızca birkaçıdır. Bu cihazlar mahremiyete yönelik önemli bir endişe kaynağıdır ve bu çerçevede mahremiyeti sağlamak oldukça zordur. Ancak mobil cihazlarda güvenliğimizi sağlayacak; mesaj ve fotoğraf bilgilerini şifreleyen, web gezinme geçmişini saklayan programlar ile GPS konum tespiti kapatılması gibi temel adımlarla başlayabilirsiniz.

## İnternet Fiziksel ve Psikolojik Sağlığımız İçin Bir Tehdit mi?

İnternet birçok alanda kullanıcılarına çeşitli fırsatlar sunan; her türlü bilgi ve belgeye ulaşma imkânı sağlayan, insanların duygu ve düşüncelerini rahatça ortaya koymasına izin veren, kısacası birçok alanda hayatı kolaylaştıran önemli bir bilişim ve iletişim aracıdır. Bu araç, bu platformda sayılan birçok kısım dâhilinde bilinçli, güvenli ve etkin kullanılmadığı takdirde çeşitli yönlerden bireyin kendi kendine çeşitli zararlar verdiği, daha doğrusu internetin bireye vermiş olduğu zararlar olduğu bilinmektedir. O zaman bilgisayar ve internet kullanımının sağlık üstündeki etkilerini kısaca açıklayalım;

### 1. Fiziksel Sağlık Sorunları

Bilgi teknolojilerini kullanırken karşılaşılan en belirgin sağlık sorunları arasında fiziksel sağlık sorunları gelmektedir. Kas ve iskelet sorunlarından yeme sorunları ve obeziteye ve göz problemlerine kadar birçok fiziksel rahatsızlıkla karşılaşabilmektedir. Bu sıkıntılardan en çok karşılaşılanları;

- Boyun ve sırt ağrısı
- Ellerde ağrı ve karpal tünel sendromu
- Görme bozuklukları
- Baş ağrısı ve migren
- Özellikle çocuklarda aşırı kilo alımıdır.

### Fiziksel Sorunlarla En Az Düzeyde Karşılaşmak İçin;

- Bilgisayar başında saatler boyunca oturmaktan kaçının, küçük molalar verin, ergonomik koltuk ve sırt destekleyici esnek malzemeler kullanmaya özen gösterin.
- Fazla eğilmeden dik bir şekilde masanızda oturmaya çalışın ve masa-sandalye duruşunu iyi ayarlayın.
- Bilgisayar ekranının üs kenarı göz seviyesini aşmamalıdır.
- Gözleri dinlendirmek için 45 dakika ekran karşısında geçirildikten sonra 15 dakika gözleri yormayacak, daha az dikkat gerektirecek aktiviteler yapın.
- Otururken dizlerinizi hafiften yukarıya, bel hizasının üzerine doğru hareket ettirin ve tüm vücudunuzun hareket etmesini sağlayın.
- Bilgisayar başında sürekli yazı yazıyorsanız bazı parmak egzersizleri yapın ve kollarınızı ara sıra dikine uzatıp çekin.
- Aşırı kilo alımı ve diğer fiziksel problemlerin önüne geçmek için her şeyden önce günlük fiziksel hareketinizi artırın, haftada en az 4 kez ve en az yarım saat egzersiz ve spor yapmaya çalışın. Fiziksel rahatsızlıkların önüne geçmek için yürüyüş ve yüzme en ideal sporlardandır.
- Fizik tedavi doktorunuzla iletişiminizi koparmayın ve doktorunuzun dediklerine riayet edin.



## 2. Psikolojik Sağlık Sorunları

Fiziksel rahatsızlıkların yanı sıra psikolojik sağlık sorunları belki de fiziksel rahatsızlıklar kadar kolay anlaşılamayan ve tedavi yöntemi daha zaman alıcı ve zor olan sorunlardır. Başlıca psikolojik rahatsızlıklar;

- Anksiyete (kaygı) bozukluğu
- İçer dönüklük, stres, asosyallik ve depresyon
- İnternet bağımlılığı

İnternet kullanımına bağlı gelişen kaygı bozukluğu aynı zamanda öfke ve şiddet davranışlarına da neden olabilir. Özellikle şiddet unsurları içeren siteler, şiddeti ve çeteleşmeyi özendiren sosyal ağlar ve şiddeti, yıkımı başarı olarak tanımlayan site ve oyunlar çocukların duygu durumlarında değişimlere sebebiyet verebilmektedir.

Çocuğun özellikle sosyal ağlarda kendisini olduğu gibi yansıtmaması nedeniyle kimlik karmaşası yaşamasına, sanal arkadaşlıklar ve ilişkiler çocuğun kalabalık bir sanal ortamda kendini yalnız hissetmesine neden olabilmektedir. Stres, içer dönüklük ve depresyonla başa çıkmak için birey olabildiğince olumlu düşünmeli, bilgisayar ve internet başında geçirdiği vakti sınırlandırmalı, sosyal aktivitelere yeterince vakit ayırmalıdır



### Ebeveynler Nelere Dikkat Etmeli?

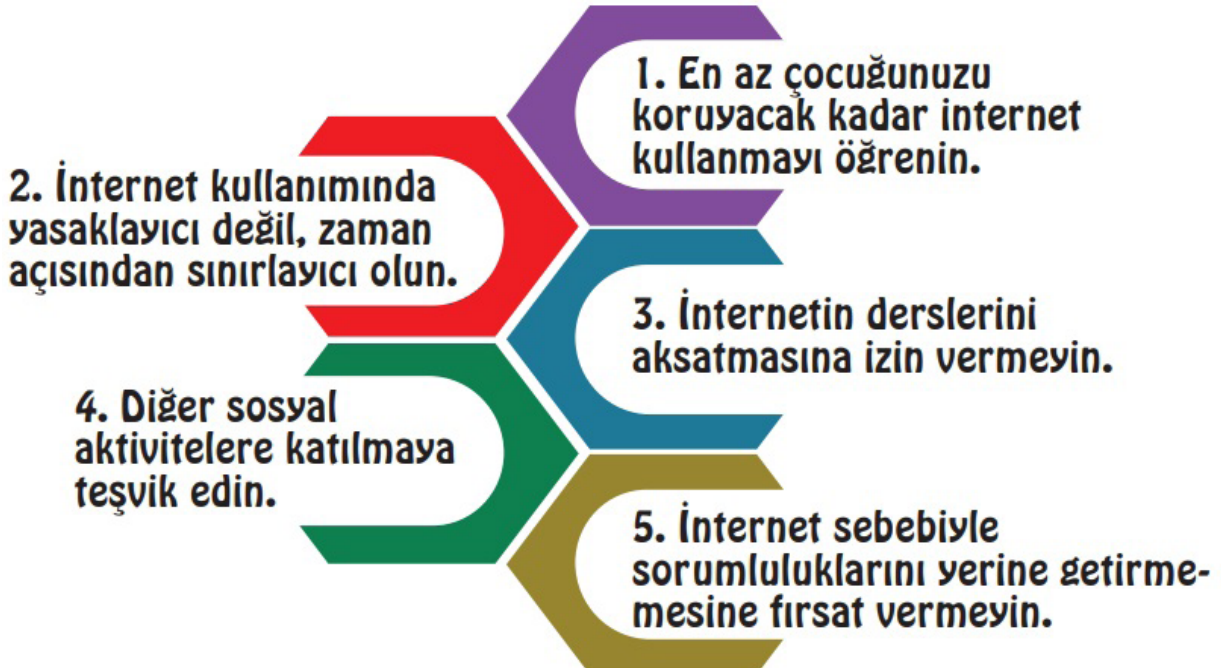
✓ **Kararlılık ve Kurallar:** Ebeveynlerin kararlılığı teknoloji kaynaklı pek çok zararı bertaraf eder. Ebeveynler çocukları için kurallar belirlemeli, ekran başında geçirilen zamana mutlaka bir sınır konulmalıdır.

✓ **İletişim ve Bağlar:** Günümüzde yüz yüze iletişim, korunması ve değer verilmesi gereken bir değer konumundadır. Çocuğuyla iletişim kurmak isteyen bir ebeveyn çocuğu ile göz kontağı kurmalıdır.

✓ **Fiziksel Hareket:** Günümüzde fiziksel aktivite çocuklarımız için hayati bir önem taşımaktadır. Fiziksel hareket çocukların genel sağlığı ve zihinsel gelişimi için çok önemlidir. Ekran başında geçirilen zamanlar arttıkça çocuklar fiziksel ve zihinsel olarak daha pasif olmakta bu da obezite ve diğer sağlık sorunlarına sebep olabilmektedir.

✓ **“Geri-Pas Etkisi”:** Carly Schuler tarafından ortaya atılan bu terim, ebeveynlerin bekleme odalarında, restoranlarda, evde çocuklarını eğlendirmek, eğitmek ya da sakinleştirmek için onlara kendi dijital cihazlarını vermesi anlamına geliyor. Yani ebeveynlerin teknolojiyi bir çeşit “duygusal emzik” olarak kullanmaları durumu. Zamanın hızlı temposu içinde bazen ebeveynler çocuklarını sessiz tutmak, oyalamak veya zaman kazanmak için çocukları teknolojik cihazlarla ve ekranlarla gönüllü ve uzun süreler baş başa bırakabiliyor. Bunu hemen her ebeveyn yaşamış olsa da ilk ve tek çare bu olmamalıdır. Ebeveynler çocuklarını sakinleştirme konusunda sağlıklı ve güçlü iletişimler kurarak, problemleri durumlarda fiziksel aktivitelere yönlendirerek ve sorun çözme konusunda bilimsel yöntemler hakkında bilgi sahibi olarak bu sorunu aşabilirler.

✓ **Uyku ve Oyun:** Çocukların hem geleneksel hem de dijital oyun oynamaya ihtiyacı vardır. Günlük hayatın akışı içinde gerçekleşecek açık hava oyunları çocuklar için çok önemlidir. Dijital dünyada oyun oynayarak geçirilen süre ile, gerçek hayatta insanlarla etkileşim halinde oynanan oyunlar arasında bir denge sağlanmalıdır.



## Popüler Bir Dijital Sorun: Cinsel Sömürü ve Mesajlaşma

**✓ Sömürü Nedir:** Bir bireyin başka bir bireyden faydalanması ya da adil olmayan bir biçimde başkası üzerinden avantaj sağlamasına sömürü denmektedir. Cinsel sömürü ise; hassas bir durumun, güç ilişkisinin veya güvenin cinsel amaçlarla fiili olarak istismar edilmesi veya istismar edilme girişiminde bulunulmasıdır.



### Bazı Cinsel Sömürü Biçimleri:

- 1- Çocuğun maddi ya da başka bir yarar karşılığı cinsel etkinliklerde kullanılması,
- 2- Çocuğun “hangi yoldan olursa olsun, belirleyici özelliği cinsel amaçlı bir betimleme olmak üzere çocuğu gerçek fiille ya da benzeştirme yoluyla cinsel etkinlik içinde gösterme ya da çocuk bedeninin herhangi bir biçimde teşhiri.



Yüz yüze ilişkilerin git gide azaldığı günümüzde, her konu internet ortamına taşınabilir ve orada tartışılabilir bir hal almış durumda. Çocuklar için engin bir bilgi kaynağı olan internet,

çocukların her türlü sorularını yanıtlayabilmenin yanı sıra onlara yaratıcılıklarını geliştirecek pek çok imkan da sağlıyor. Bunların dışında, dijital ortamda çocukların korunması ve kontrol edilmesi gereken durumlar da var. Normal yaşamda olabileceği gibi çocuğa yönelik cinsel saldırılar internet üzerinden de gerçekleşebiliyor. Bunun bir yansıması olarak dijital dünyada karşımıza cinsel içerikli mesajlaşma kavramı çıkıyor.

Cinsel içerikli mesajlaşma, mesajlaşmak anlamına gelen 'texting'den geliyor. Sosyal medya ve diğer dijital medya uygulamaları üzerinden cinsel içerikli fotoğraf ve bilgi paylaşımı anlamına gelen cinsel içerikli mesajlaşma, günümüzde çocukları için büyük sorun haline gelmiş durumda. Cinsel içerikli mesajlaşma, Facebook, Twitter ve Instagram gibi sosyal medya ortamları aracılığıyla da gerçekleştirilebilmekte. Bunlara ek olarak örnekleri ülkemizde de yaygın olarak görülen, sanal ortamda çevrimiçi oynanan oyunlarda da çocuklar cinsel içerikli paylaşım yapmaya veya konuşmaya zorlanabiliyorlar.

Bu durum, yalnızca çocuklar arasında gerçekleşen bir şey değil aynı zamanda bazı yetişkinler tarafından çocuklara yönelen bir tehdit olarak da görülmektedir. Bütün bunlar göz önünde bulundurulduğunda, cinsel içerikli mesajlaşma, aileler tarafından çok dikkat edilmesi gereken bir durum haline geliyor.

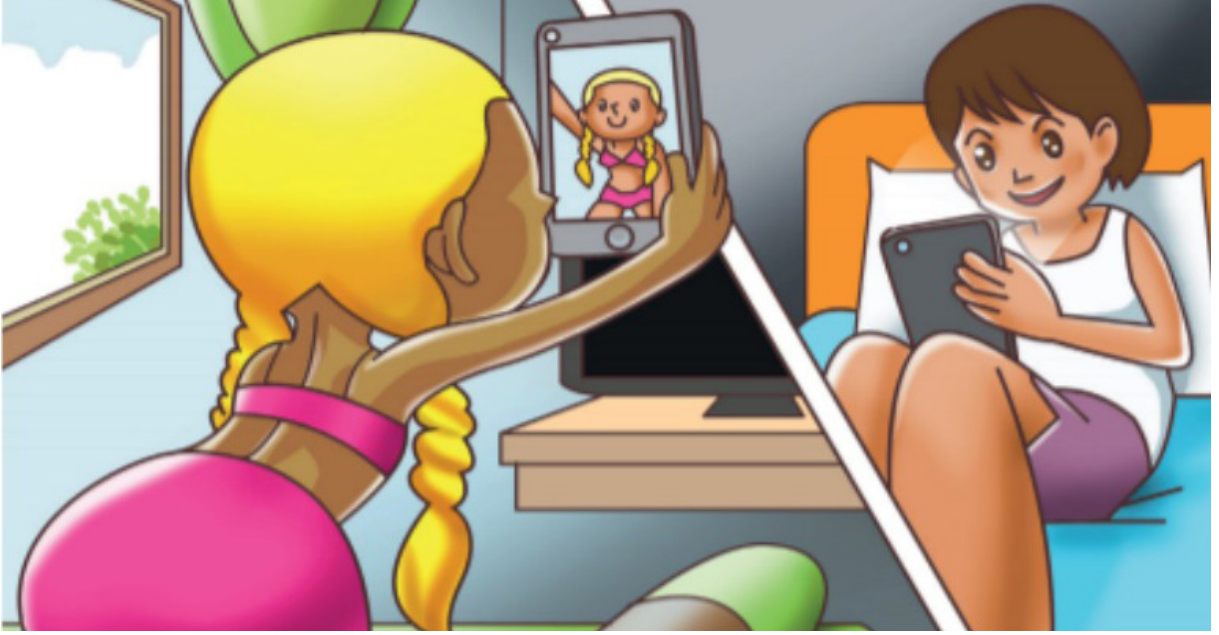


Yapılan araştırmalar her 10 gençten 6'sının çocukluk dönemlerinde cinsel içerikli mesaj ya da görseller göndermesi yönünde taleplere maruz kalabildiğini gösteriyor.

Aynı araştırmalar özellikle kız çocuklarının buna daha çok zorlandığını ortaya koyuyor. Özellikle ergenlik süreçlerinde beğenilme ve kendini beğendirme arzusunun da etkisiyle kendine dair fotoğraflara yönelik eleştiriler kişilik ve özgüveni olumsuz etkiliyor. Cinsel içerikli mesajlaşma, aynı zamanda sanal zorbalığın yüksek oranda görülebileceği bir mekanizma olarak ifade ediliyor.

Çocuğun kendine olan güveninin kırılmasına neden olacak geri dönüşler, özellikle gençler arasında intihara kadar gidebiliyor. Bunların ötesinde, yaşça büyük biri tarafından bu şekilde istismara uğrayan çocuk ciddi anlamda psikolojik olarak etkilenmesinin dışında yardıma da ihtiyaç duyuyor.

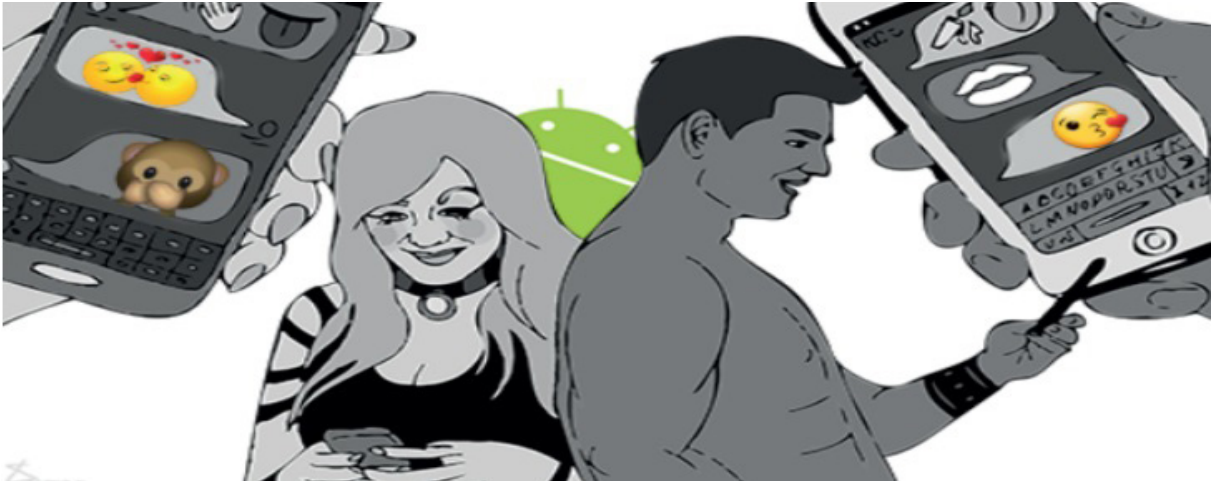




Çocuk Hakları Sözleşmesinin Çocuk Güvenliği Hakkındaki Seçmeli Protokolü'ne göre çocuk pornografisi, hangi yoldan olursa olsun, belirleyici özelliği cinsel amaçlı bir betimleme olmak üzere, çocuğu gerçek fiille ya da benzeştirme yoluyla cinsel etkinlik içinde gösterme ya da çocuğun bedenini herhangi bir biçimde teşhir anlamına gelir. Bu tanım cinsel içerikli mesajlaşmanın unsurlarını kapsayabilmesi için dikkate alınmalıdır. Sonuç olarak, cinsel içerikli görüntüyü kaydeden ve/veya gönderen kişi, müstehcenlik(pornografi) ile ilgili yasa maddesini ihlal etmekten dolayı yargılanabilir. Buna ek olarak, bu mesajı alan kişi de bu müstehcen görüntüye erişmek ve/veya bu materyali bulundurmamak suçundan yargılanabilir.

### Aileler Ne Yapmalı?

12 yaş ve üstündeki çocukların özellikle kendilerini keşfetmeye başlamaları, günlük hayattaki ilişkilerinin de yeni bir boyut kazanmasını sağlıyor. Bu nedenle cinsel içerikli mesajlaşma hayatlarına daha kolay bir şekilde giriyor. Burada ailelere büyük bir rol düşüyor ve önemli olan nokta, çocuklarla empati yaparak aile içi diyalogu yüksek tutmak.



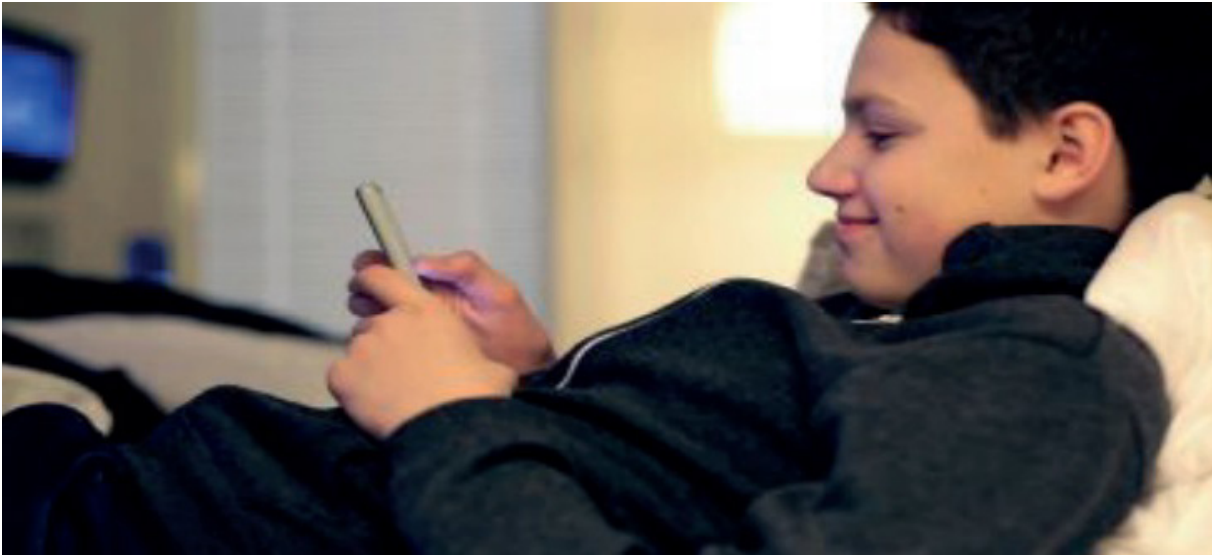
Ailelerin çocuklarını kesin bir şekilde koruması ve gözlemlemesi gerektiği konu ise yaşça büyük kişiler tarafından çocuğun cinsel içerikli mesajlaşmaya maruz kalmasıdır. Çocuğunuzla oturup bu konu hakkında konuşurken, çocuğunuzun mağdur tarafta veya bu davranışı

karşılıklı yapan tarafta olmasının bir önemi yoktur. Çocuğunuzla cinsel içerikli mesajlaşma konusunda konuşmanız, onu en etkili şekilde bundan korumanızı sağlayacaktır. Karşı tarafa müstehcen bir paylaşımda bulunduğunda neler olabileceği konusunda “yaşını da dikkate alarak” en açık şekilde konuşabilirsiniz. Ona ‘gönder’ tuşuna baktıktan sonra görüntünün kontrolünün artık onda olmayacağını, göndereceği kişinin kontrolü altında olacağını anlatın.

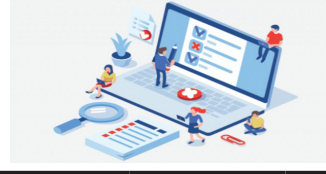
Yine yaşını göz önünde bulundurarak, bu şekilde görüntü gönderip almanın veya bulundurmanın yasal olmadığını, bunun suç teşkil edebileceğini izah edin.



Bütün bunları yaparken dikkat edilmesi gereken, iletişim kurmak ve konuyu kabullenip, çocuğunuza cinsel içerikli mesajlaşmanın risklerini en doğru şekilde anlatmak. Bunların dışında, çocuğunun böyle bir durumla karşı karşıya kaldığını fark eden ebeveynlerin, doğrudan polise başvurup adli süreci başlatmaları ve rapor etmeleri gerekir. Cinsel içerikli mesajlaşma günümüzde, teknolojinin gelişmesiyle çocuk istismarının farklı bir görüntüye bürünmüş hali oldu. Bununla başa çıkmak bütün ebeveynlerin sorumluluğunda. Bu nedenle, mağdur olan çocuğu ikinci kez mağdur etmeden hukuki sürecin başlatılması en doğrusudur.



## Sağlıklı Dijital Yaşam Kontrol Listesi



| Sevgili Veliler ve Öğrenciler,<br>Lütfen Kontrol Listesinin tüm maddelerini dikkatlice okuyup birlikte işaretleyiniz!                                                     | İşaret Alanı | Açıklama |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|----------|
| 1- İnternet ortamlarından edindiğim bilgilerin doğru olup olmadığını veya en azından güvenilir olup olmadığını teyit ediyorum.                                            |              |          |
| 2- İnternet ortamlarında paylaştığım haber veya bilgilerin doğru olup olmadığını veya en azından güvenilir olup olmadığını kontrol ediyorum.                              |              |          |
| 3- İnternet ortamlarında kullandığım program veya sistemlerin şifreleme ve güvenlik ayarları konusunda yeterince bilgiye sahibim.                                         |              |          |
| 4- İnternet ortamlarında kullandığım program veya sistemlerin gizlilik ayarları konusunda yeterince bilgiye sahibim.                                                      |              |          |
| 5- Çevrim içi karşılaştığım ve beni üzen veya rahatsız eden durumları tanımlayabiliyor ve bunlarla mücadelede uygun yöntemlerin neler olduğunu biliyorum.                 |              |          |
| 6- Çevrim içi karşılaştığım ve beni üzen veya rahatsız eden durumlarda gerektiğinde hangi kişi ve kurumlarla irtibata geçmem gerektiği konusunda yeterli bilgiye sahibim. |              |          |
| 7- Mahremiyet ve etik hakkında bildiklerim, internet ortamlarından edindiğim bilgiler gibi kişisel çevrimiçi eylemlerimi kontrol etmeme yardımcı olacak düzeyde.          |              |          |
| 8- Mahremiyet ve etik hakkında bildiklerim, internet ortamlarındaki paylaşımlarım gibi kişisel çevrimiçi eylemlerimi kontrol etmeme yardımcı olacak düzeyde.              |              |          |
| 9- İnternet kullanımım gündelik yaşamdaki (okul, ev, iş vb.) başarıyı olumlu yönde etkiliyor.                                                                             |              |          |
| 10- Çevremdeki insanlarla ilişkilerimin internet kullanımımından etkilenmemesini sağlıyorum.                                                                              |              |          |
| 11- İnterneti dengeli ve sağlıklı olmayan bir biçimde kullanmamın fiziksel sağlığıma etkileri konusunda yeterli bilgiye sahibim.                                          |              |          |
| 12- İnterneti dengeli ve sağlıklı olmayan bir biçimde kullanmamın psikolojik sağlığıma etkileri konusunda yeterli bilgiye sahibim.                                        |              |          |

**Not: Kendinizi yetersiz hissettiğiniz durumlarda bu kitapçığın ilgili bölümlerine yeniden bakabilir, daha ileri bilgi ve okumalar için <http://hdlife.erciyes.edu.tr/> adresini ziyaret edebilirsiniz.!**

## Sağlıklı Dijital Yaşam Sözleşmesi



Sevgili Veliler ve Öğrenciler;

Bu sözleşmenin amacı, sizlere dijital aktivitelerinizde bilinçli-akıllı, sorumlu ve saygılı olmaya yönlendiren bir yol açmak ve onların arkasındaki etik sonuçları anlamanıza yardımcı olmaktır.

Lütfen sözleşmenin tüm maddelerini dikkatlice okuyup birlikte değerlendiriniz!

- 1- İnternet ortamlarından edindiğim veya aynı ortamlarda paylaştığım haber veya bilgilerin gerçek olup olmadığını dikkatlice araştıracağımı;
- 2- İnternet ortamlarında kullandığım program veya sistemlerin şifreleme, güvenlik ve gizlilik ayarları konusunda gerekli bilgileri edineceğimi;
- 3- İnternette karşılaştığım ve beni üzen veya rahatsız eden durumlar konusunda ailemi ve öğretmenlerimi bilgilendireceğimi;
- 4- İnternette karşılaştığım ve beni üzen veya rahatsız eden durumlarla mücadelede uygun yöntemleri kullanmak için gerektiğinde uzman görüşüne ve güvenlik birimlerine başvuracağımı;
- 5- Mahremiyet ve etik hakkında, internet ortamlarından edindiğim bilgiler veya aynı ortamlardaki paylaşımlarım gibi kişisel çevrimiçi eylemlerimi kontrol etmeme yardımcı olacak düzeyde bilgi edineceğimi;
- 6- İnternet kullanımımı gündelik yaşamdaki (okul, ev, iş vb.) başarıyı olumlu etkileyecek yönde düzenleyeceğimi;
- 7- İnternet kullanımımın gündelik yaşamdaki (okul, ev, iş vb.) başarıyı hangi durumlarda olumsuz etkileyeceğine dair ayrıntılı bilgi edineceğimi;
- 8- İnternet kullanımımın çevremdeki insanlarla ilişkilerimi sınırlı hale getirmeyeceğini;
- 9-İnternet ortamında herhangi bir kimseye zarar verebilecek, konusu suç teşkil edebilecek metin ve multimedia içerikleri yayınlamayacağımı;
- 10-Kendi kişisel verilerime verdiğim önem kadar diğer kişilerin kişisel verilerine de önem vererek izinsiz ve yetkisiz olarak internet ortamındaki verilere erişim sağlamayacağımı;

KABUL VE TAAHHÜT EDERİM;

Adı ve Soyadı:

Yaşı:

Tarih:

İmza:





### Yararlanılan Kaynaklar:

1. İnternetteki Bilgi Ne Kadar Güvenilir: Erişim Tarihi: 15 Ağustos 2019; <https://www.dunya.com/kose-yazisi/internetteki-bilgi-ne-kadar-guvenilir/11255>
2. İnternette Güvende Kalmak: Erişim Tarihi: 15 Ağustos 2019; <https://www.guvenliweb.org.tr/blog-detay/internette-guvende-kalmak>
3. İnternet ve Sağlık: Erişim Tarihi: 15 Ağustos 2019; <https://www.guvenliweb.org.tr/dokuman-detay/internet-ve-saglik>
4. Siber Zorbalık Nedir? Nasıl Mücadele Edilir? Erişim Tarihi: 15 Ağustos 2019; <https://www.guvenliweb.org.tr/dosya/5ok8W.pdf>
5. Siber Zorbalık: Erişim Tarihi: 15 Ağustos 2019; <https://www.guvenliweb.org.tr/dokuman-detay/siber-zorbalik>
6. Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı Broşürlerimiz: Erişim Tarihi: 15 Ağustos 2019; <https://www.egm.gov.tr/siber/brosurlerimiz>
7. İnternet Bağımlılığı ve Alışkanlıklara Etkisi: Erişim Tarihi: 15 Ağustos 2019; <https://www.guvenliweb.org.tr/blog-detay/internet-bagimlili-gi-ve-aliskanliklara-etkisi>
8. Dijital Dünyada Çocuklarımızı Nasıl Büyütelim: Erişim Tarihi: 15 Ağustos 2019; <https://www.guvenliweb.org.tr/blog-detay/dijital-dunyada-cocuklarimizi-nasil-buyutelim>
9. Dijital Oyunlar ve Bireyler Üzerindeki Etkileri: Erişim Tarihi: 15 Ağustos 2019; <https://www.guvenliweb.org.tr/blog-detay/dijital-oyunlar-ve-bireyler-uzerindeki-etkileri>
10. 10 Adım: Erişim Tarihi: 15 Ağustos 2019; <https://www.guvenliweb.org.tr/dosya/SPy09.jpg/indir>
11. Dijital Mahremiyetimizi Nasıl Koruyacağız? Erişim Tarihi: 15 Ağustos 2019; <http://btdestek365.com/?p=1565>
12. Yeni Dijital Tehlike Sexting: Erişim Tarihi: 15 Ağustos 2019; <https://dijitalmedyavecocuk.bilgi.edu.tr/2017/12/14/yeni-dijital-tehlike-sexting/>
13. ÇAÇAV Online Cinsel Sömürü: Erişim Tarihi: 15 Ağustos 2019; <http://cacav.net/wp-content/uploads/2018/12/ÇAÇAV-Online-Cinsel-Sömürü.pdf>
14. Siber Zorbalık: Erişim Tarihi: 15 Ağustos 2019; <https://www.internetyardim.org.tr/siber-zorbalik/ebeveynler-a-ileler-siber-zorbalikla-mucadele-icin-neler-yapabilir>

**HD-LIFE**  
**PROJECT**

