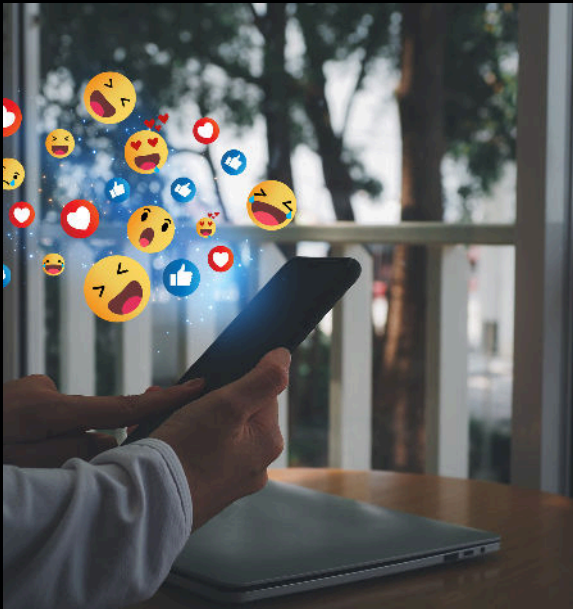


# GÜVENLİ İNTERNET VE SOSYAL MEDYA KULLANIMI

BİLİŞİM ,TEKNOLOJİ,GAZETE

İNTERNET VE  
SOSYAL MEDYA  
KULLANIMINDA  
UYULMASI  
GEREKEN  
KURALLAR...



# ADIM ADIM GÜVENLİ İNTERNET

## BİLİNÇLİ VE GÜVENLİ İNTERNET KULLANIMI İÇİN GEREKLİ 6 MADDE

1

### DOĞRULA:

İnternet'ten edindiğin her bilgi doğru olmayabilir.

2

### İNANMA:

İnternette konuştuğun kişiler, kim oldukları hakkında sana yalan söylüyor olabilir.

3

### KABUL ETME:

Tanımadığın ve güvenmediğin insanlardan gelen e-posta, mesaj, resim veya dosyaları kabul etme ve açma.

4

### KİŞİSEL BİLGİLERİNİ PAYLAŞMA:

İnternette kişisel bilgilerinin paylaşırken çok dikkatli ol.

5

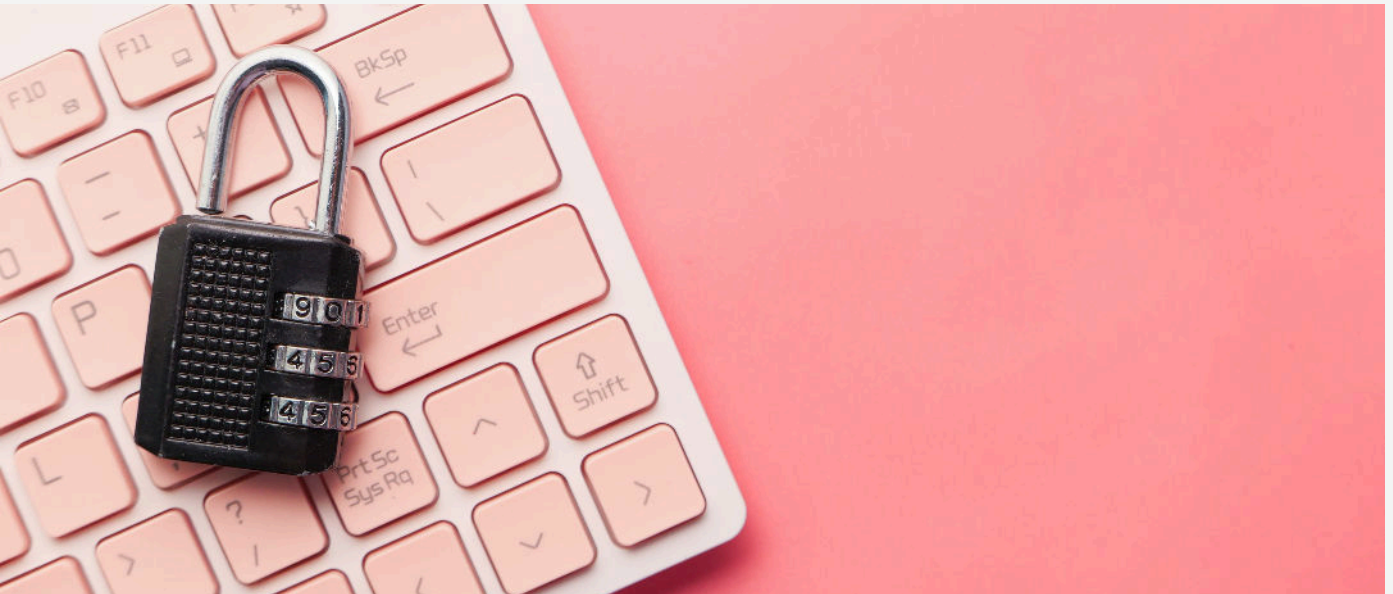
### AİLENE ANLAT:

Bulduğun yer, telefon, şifren gibi kişisel bilgilerini asla kimseyle paylaşma ve güvenli kal.

6

### TÜRKÇEYİ DOĞRU KULLAN:

Güzel Türkçemizi koru ve doğru kullan.  
Anlamsız kısaltmalar, yabancı kelimeler, bozuk cümleler kulanma.



# AİLELER İÇİN GÜVENLİ İNTERNET KULLANIMI

- 1) Kendinizi eğitin, interneti öğrenin
- 2) İnternet kullanımını ile alakalı aile içi kurallar belirleyin
- 3) Çocuğunuzu uygun bir şekilde uyarın
- 4) Oynadığı bilgisayar oyunları gözetiminizde olsun
- 5) Çocuğunuzun girdiği internet sitelerini kontrol edin
- 6) Her şeye inanmaması konusunda uyarın
- 7) Kişisel ve ailevi bilgileri paylaşmaması konusunda uyarın
- 8) Çocuğunuzla bağlantınızı koparmayın





## ÇOCUKLARINIZ İNTERNETTE GÜVENLİ Mİ?

İnternette karşılaşılması muhtemel tüm tehditlerin kokeninde gerçek hayattaki tehditler vardır. İnternet için var olan tüm risk başlıkları gerçek hayatta da karşılaşılabilecek durumlardır.

Dolayısıyla çocuklarımızı nasıl gerçek hayattaki tüm bu tehlikelerden korumak için çaba harcıyor ve kurallar koyuyorsak interneti de bilinçli, güvenli ve etkin bir şekilde kullanmayı öğrenerek ve çocuklara bunu öğreterek, sanal dünyanın risklerini minimize edebilir ve eğitim, iletişim ve güzel zaman geçirme gibi katkıları çocuklarımıza fırsat olarak sunabiliriz.

Aynı zamanda ebeveyn denetimli hesaplar kullanılarak çocuklarımızın güvenli bir şekilde internette bulunmasını sağlayabilirsiniz.

# KVKK NEDİR

2010 yılında yapılan Anayasa değişikliği ile Anayasanın özel hayatın gizliliğini düzenleyen 20. maddesine belirtildiği gibi temel bir hak olarak düzenlenen kişisel verilerin korunmasını isteme hakkı, Anayasanın kişinin hak ve ödevlerine ilişkin bölümünde yer almıştır. Aynı şekilde kişisel verilerin korunmasına ilişkin hak Anayasada çizilen sınırlar çerçevesinde diğer hak ve özgürlükler lehine sınırlandırılabilir. Avrupa Birliğine uyum kapsamında hazırlanan Kişisel Verilerin Korunması Kanunu Tasarısı 18 Ocak 2016 tarihinde TBMM Başkanlığına sevk edildi.

Bugün ülkeler, kurumlar, şirketler hatta bireyler iş veya eğlence araçları nedeniyle hızla dijitalleşmeye başlamış, ardından da bilgi herkes için çok daha önemli bir hale gelmiştir. Bilgiye erişim kolaylaştıkça kötü niyetli kişilerin dikkatini çekmiş, bilginin değeri arttıkça da saldırıların artmasına sebep olmuştur. Teknoloji bilgiye erişimimizi çok daha kolay bir hale getirdiği gibi, saldırganların da yeni teknikler ve yeni metotlar kullanabilmesine olanak sağlamıştır.



# 5 ADIMDA

## Kişisel Veri Güvenliğini Nasıl Sağlarsın?

1

### Tıklamadan önce düşün!

Paylaşmak istediğin fotoğrafları, yorumları, mesajları ve videoları internet ortamına yüklemeyen önce bir kez daha düşün.

PAYLAŞ



2

### Paylaştığın şeylerin gizli kalmayacağını hatırla!

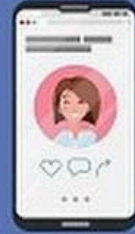
İnternet ortamında paylaştığın yorumlar, mesajlar, fotoğraflar ve videolar kopyalanabilir ve başkalarına gönderilebilir.



3

### Gerçekten arkadaşın mı?

İnternet ortamında arkadaş olduğun kişilerin gerçek kimliğini bilemezsin.



4

### Gizliliğini şifrelerle koru!

Mobil cihazlarda şifre güvenliği önemlidir; hesaplarınızı korumak için güçlü şifreler oluşturun ve başkalarıyla paylaşmayın.



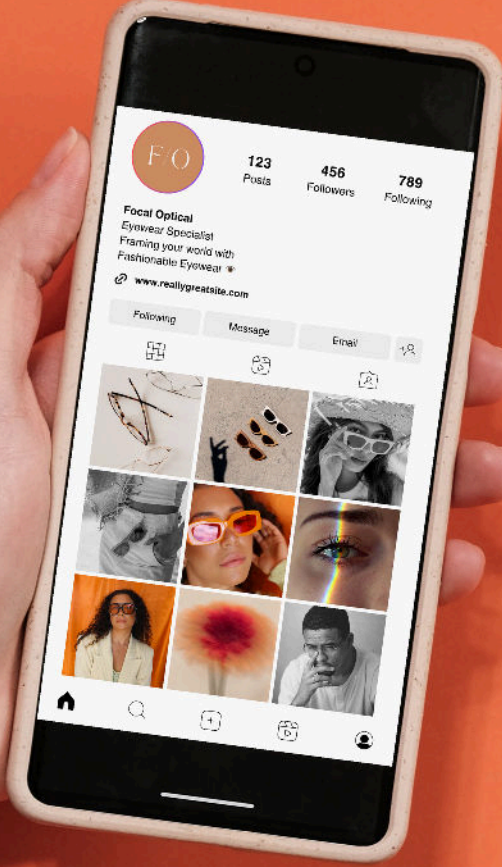
5

### Arkadaşlarının hakkına saygı göster!

Başkalarının da bulunduğu fotoğraf veya videoları paylaşmadan önce bu paylaşımın onlar için sorun olup olmadığını sor ve internet ortamında başkaları hakkında söylediklerini dikkatlice düşün.



Aslında çoğu şey gerçek dünya ile aynı. Aynı konular konuşuluyor, paylaşılıyor. Cümleler, istekler, sorular, sorunlar aynı. Farklı olan ise ortamın özelliği. Normalde; sınıfta, bahçede, parkta yapılan ve herkesin birbirini tanıdığı, bildiği sohbetler artık sanal ortamlarda yapılıyor. Mesafe, sınır, kural, ihlal, etik gibi bir çok kavram ya hiç yok ya da farklı şekilde çıkıyor karşınıza. Sosyal Medya renkli, hareketli ve eğlenceli bir dünya. Kullanıcıların hoş vakit geçirdiği, yeni kişiler tanıdığı, fikirlerini özgürce ifade ettiği bir ortam. Bununla birlikte, bilinçli kullanılmadığı vakit birçok soruna yol açan bir yapısı da var aslında. Sosyal medyanın etkisinden kaçamıyorsak en iyi yol bu yeni iletişim aracını bilinçli kullanmaktır.



## SOSYAL MEDYA NEDİR?



# SOSYAL MEDYANIN GÜVENLİ KULLANIMI

## 1. Güçlü parolalar kullanın

Parolalar, güvenlik açısından ilk savunma hattıdır. Tüm hesaplarınızda güçlü ve benzersiz olmalıdır. Parolalarınız en az 8 karakter uzunluğunda olmalıdır. Harfler, rakamlar ve özel karakterler içermelidir. Ayrıca, şifrelerinizi sık sık değiştirmeli ve onları sadece sizin bildiğiniz bir yöntemle saklamalısınız. Kısa şifreler belirleyerek birçok hesapta aynı şifreyi kullanmak çok pratik olsa da doğru değildir. Her hesabınız için farklı ve güvenli şifreler oluşturmalısınız.

## 2. İki faktörlü kimlik doğrulama kullanın

İki faktörlü kimlik doğrulama, parolanızın yanı sıra doğrulama kodunun da gerektiği güvenlik özelliğidir. Bu özellik sayesinde hesabınıza giriş yaptığınızda, doğrulamak için rastgele oluşturulmuş bir kod gönderilir. Hesabınıza erişmek isteyen başka kişilerin bu koda ulaşması mümkün olmayacağı için daha güvenli olacaktır. Bu doğrulama kodu, genellikle telefonunuza SMS olarak gönderilir veya bir uygulama aracılığıyla ulaşır. İki faktörlü kimlik doğrulama, hesabınıza erişimi daha zor hale getirir ve hesabınızın güvenliğini artırır.



### 3. Hesap ayarlarınızı güncel tutun

Hesap ayarlarınızı güncel tutun ve güvenlik ayarlarınızı düzenli olarak kontrol edin. Örneğin, parolanızı değiştirirseniz veya yeni bir cep telefonu numarasına sahip olursanız, bu bilgileri hesap ayarlarınızda güncelleyin. Ayrıca, hesabınızın güvenlik ayarlarını düzenli olarak kontrol edin ve gerekirse değiştirin.

### 4. Özel bilgilerinizi paylaşmayın

Parolanız ve finansal bilgileriniz gibi özel bilgilerinizi kimseyle paylaşmayın. Bu bilgiler, sizi takip edenler tarafından kötü niyetli olarak kullanılabilir veya çalınabilir. Ayrıca, bu bilgileri güvenli bir şekilde saklayın. Örneğin, parolanızı ya da kişisel bilgilerinizi herkesin kolayca erişim sağlayabileceği bir bilgisayar dosyasında saklamayın.

### 5. Güvenilmeyen bağlantılardan ve e-postalardan uzak durun

Güvenilmeyen bağlantıları ve e-postalardaki açmayın. Bu bağlantılar genellikle phishing (oltalama) saldırılarının bir parçası olabilir ve sizin bilgilerinizi ele geçirmeyi amaçlar. Güvenilmeyen bir e-posta alırsanız, bu e-postanın gerçek olup olmadığını kontrol edin. Örneğin, bankanızın adını ve logosunu kullanan bir e-posta alırsanız, bu e-postanın gerçek olup olmadığını doğrulamak için bankanızla iletişim kurabilirsiniz.

### 6. Bilgisayarınızda Antivirüs Programı Kullanın

Güncel bir antivirüs programı kullanarak birçok güvenlik tehdidini önlemek ve ortadan kaldırmak mümkün. Antivirüs programları hem sosyal medya hem de veri güvenliği için etkili yöntemler arasında yer almaktadır.



**SOSYAL MEDYANIN  
GÜVENLİ KULLANIMI**