

# SİBER ZORBALIK

Bilişim teknolojileri ve iletişim teknolojilerini kullanarak yapılan zorbalıktır. BİT' i kullanarak bir birey ya da gruba karşı yapılan teknik ya da ilişkisel tarzda zarar verme davranışlarının tümüdür. Gerçek hayatta suç sayılan hakaret, iftira, dolandırıcılık, taciz, küfür gibi zorbalık davranışları sanal ortamda da suç sayılır ve siber suçlar kapsamına girer. Sanal ortamda bu haklarımız kanunlar ile korunur.

## İnternet Kullanırken Dikkat Edilecek Hususlar

- T.C. kimlik, adınızı soyadınızı, adresinizi, tanımadıklarınızla paylaşmayın
- Banka gibi online kullanılan sitelerin kullanıcı adı ve şifrelerini başkalarının bilmesini engellemeliyiz
- Sosyal paylaşım alanlarında kişisel bilgilerimizi herkese açık tutmamalıyız.
- Yaşımıza uygun siteleri kullanmalıyız
- Sosyal paylaşım alanlarında tanımadığımız kişileri samimi sanıp muhabbet etmemeliyiz. Ekranın arkasındaki kişiler belki sandığımız kişiler değildir bunu unutmamalıyız.
- Şifre ile girdiğimiz sitelerden "Güvenli Çıkış" tıklayarak çıkmalıyız.
- Siber zorbalığa maruz kaldığımızı anladığımızda büyüklerden veya öğretmenlerimizden destek almalıyız.
- İnternet bağımlılığına yönelik kendimiz ve ailemiz adına önlem almalıyız.
- Başlıklar hariç büyük harf yazı yazmayın. Büyük harf BAĞIRMAK anlamındadır.
- Karışık harflerle yazmayın, jhdgajhls KÜFÜR anlamındadır.

## ZARARLI YAZILIM

Çoğu zaman bu zararlı yazılımların hepsine virüs deyip geçiyoruz ama aslında birbirlerinden farklılar ve kimi zaman yazılımın türüne göre özel önlem veya işlem yapmak durumunda kalabiliyoruz.

## ZARARLI YAZILIM TÜRLERİ

### Virüs Nedir?

Virüs, bilgisayarınıza girip dosya ya da verilerinize zarar verir, tahrif eder. Virüsler bilgisayarınızda verileri bozabilir hatta silebilir. Ayrıca kendilerini çoğaltabilirler (gerçek virüsler gibi). Bilgisayar virüsü pek çok zararlı yazılımdan çok daha tehlikelidir çünkü doğrudan dosyalarınıza ve verilerinize zarar verirler.

### Truva atı (Trojan) Nedir?

Truva atı bir virüs değildir. Gerçek bir uygulama gibi gözükür zararlı bir program türüdür. Trojan kendini çoğaltmaz ama virüs kadar yıkıcı olabilir. Truva atı bilgisayarınıza güvenlik açığı oluşturur ki bu da zararlı programların, kişilerin sisteminize girmesi için bir yol açar.

Bu şekilde kullanıcıların kişisel bilgileri çalınabilir. Yani aynı tarihteki Truva savaşındaki olduğu gibi normal bir program zannettiğiniz Truva Atı, sisteminize girer ve Grek askerlerinin ordunun girmesi için kale kapılarını içeriden açması gibi zararlı yazılımların, hackerların sisteminize girmesi için bir güvenlik açığı oluşturur.

### Solucan (Worm) Nedir?

Solucanlar yerel sürücüde ya da ağda kendini tekrar tekrar kopyalayan bir programdır. Tek amacı sürekli kendini kopyalamaktır. Herhangi bir dosya ya da veriye zarar vermez ancak sürekli kopyalama yaparak sistemi meşgul eder ve performansı etkiler. Virüslerin aksine bir programa bulaşmaya ihtiyacı yoktur. İşletim sistemlerindeki açıklardan yararlanarak yayılırlar.

## Reklam Yazılımı (Adware) Nedir?

Genel olarak Adware, herhangi bir program çalışırken reklam açan yazılımdır. Adware internette gezerken otomatik olarak bilgisayarınıza inebilir ve pop-up pencereleri ile görüntülenebilir. Kullanıcıları oldukça rahatsız eden Adware tipi uygulamalar çoğunlukla şirketlerce reklam amaçlı olarak kullanılırlar.

## Casus Yazılım (Spyware) Nedir?

Casus yazılım, kullanıcının izniyle veya izni dışında bilgisayara yüklenen ve kullanıcı, (örneğin webde gezdiği sayfalar, vb.) ya da bilgisayar hakkında bilgi toplayıp bunları uzaktaki bir kullanıcıya gönderen bir program türüdür. Ayrıca bilgisayara zararlı yazılımlar indirip yükleyebilir. Adware gibi çalışır ama çoğunlukla kullanıcı başka bir program yüklerken onun bilgisi dışında, gizli bir biçimde yüklenir.

## Spam Nedir?

Aynı mesajdan çok sayıda göndererek bir mail adresini, forumu vb. boğmaya spam yapmak adı veriliyor. Spamların çoğu reklam amaçlı oluyor ve kullanıcıların isteği dışında posta adreslerine gönderiliyor.



# SİBER TUZAKLARI NASIL ANLARIM?

- 1 İnternette kimlik bilgilerini isteyen web sitelerine karşı **dikkatli ol.**
- 2 **Bedava** hediyelerden, programlardan ve **kazanacağını söyleyen yarışmalardan uzak dur.**
- 3 Eğlenceli gibi görünen testler, **senin hakkında bilgi toplamak için** hazırlanmış olabilir. **Bir kez daha düşün.**
- 4 Unutma! Bilinen markalar veya kurumlar e-posta yoluyla senden **parola, kimlik bilgileri gibi kişisel bilgiler istemez.**
- 5 Açılır pencerelerle (**pop-up**) gelen yarışma ve anketlere **katılma.**
- 6 Şüpheli bulduğun e-postaların içindeki bağlantıya (linke) tıklama ve gönderilen dosyayı **açma.**
- 7 Tanımadığın kişilerden gelen e-postaları açmadan önce, **tekrar düşün.**
- 8 İçeriği arkadaşlarına da göndermeni isteyen e-postalar, seni ve arkadaşlarını riske atabilir. E-postayı sil ve arkadaşlarını **uyar.**
- 9 İsteğin dışında bilgisayar kameranın açılmaması için, kameranı **kontrol et.**
- 10 Oyun oynamak için, **üye olmanı isteyen siteleri önce dikkatlice incele.**