

## ÜNİTE 2

### ETİK VE GÜVENLİK

Etik kelimesinin eş anlamlısı **ahlaktır**.

#### İnternet Etiği

İnterneti kullanırken uyulması ve kaçınılması gereken kuralların tamamına **internet etiği** denir. Güvenilir, dürüst ve saygılı internet ortamı için uyulması gereken kurallar vardır. Bunlardan bazıları,

1. Toplum içerisinde sergilediğiniz olumlu tavırları internet ortamında da sürdürün.
2. Kişilere istekleri dışında rahatsız olacakları iletiler göndermeyin.
3. Anlamsız ve gereksiz iletiler göndermeyin.
4. Doğruluğundan emin olmadığınız bilgileri paylaşmaktan kaçının.
5. Başkalarının kişilik haklarına ve özel yaşamlarına saygılı olun.

#### Siber Zorbalık

Bir kişi ya da grubun bilgi ve iletişim teknolojilerini, diğer kişi ya da gruplara karşı;

- Zarar vermek amacıyla,
- Kötü niyetli olarak,
- Tekrarlayan biçimde kullanmasıdır.

Siber zorbalık genellikle cep telefonu, tablet ya da bilgisayar kullanılarak sosyal medya, cep telefonu uygulamaları ve oyunlar üzerinden yapılmaktadır.



#### Siber Zorbalığa Maruz Kaldığımızda Alınabilecek Önlemler

- Sanal ortamda her zaman sorgulayıcı olmalıyız
- Şüphelendiğiniz kişi, ileti ya da istekler karşısında durumu hemen ailemize bildirmeliyiz.
- Tanımadığımız kişilerden gelen çeşitli teklifler ve davetlere karşı dikkatli olmalı, şüpheli davranmalıyız.
- Telefon numarası, adres, kimlik bilgileri gibi özel bilgileri kesinlikle başkaları ile paylaşmamalıyız.
- Kredi kartı ve banka kartı gibi bilgileri kesinlikle paylaşmamalıyız.
- Siber zorbalığa maruz kaldığımızı düşündüğümüzde, sayfada bulunan **ENGELLE** **ŞİKAYET ET** gibi butonları kullanmalıyız.



#### Telif Hakkı

Bir kişinin emği ile meydana getirdiği bilgi, düşünce, sanat eseri ve ürünün izinsiz olarak kullanılması ile ilgili hukuken sağlanan haklara **telif hakkı** denir. Sembolü ©

İnternet ortamındaki tüm verileri istediğimiz gibi kullanamayız. Kullanacağımız yazı, resim ya da videonun telif hakkı bir başkasına ait olabilir. İzinsiz kullanmak suçtur.

**NOT:** Telif hakkını ihlal etmek, başkasının ürettiği içeriği izinsiz kullanmak demektir. Telif hakkı ihlali bir suçtur. Her suç gibi telif hakkı ihlalinin de cezası vardır.

## Kullanım Haklarına Göre Yazılım Türleri (Lisans Türleri)

Kullandığımız yazılımlar, oynadığımız oyunlar ve benzeri diğer yazılımların kullanım hakkına **lisans** denir. Yazılımlar kullanım haklarına göre 4 grupta incelenir.

1. **Lisans Yazılımı:** Tüm kullanım haklarını para ile satın aldığımız yazılımlardır. Örneğin, Microsoft Windows 11, Microsoft Office programları
2. **Ücretsiz Yazılım (Freeware):** Hiçbir ücret ödemediğimiz ve indirebileceğimiz yazılımlardır. Örneğin, Google Chrome, Pardus
3. **Demo Yazılım:** Tanıtım amaçlı hazırlanmış, işlem kısıtlılığı bulunan yazılımlardır. Tüm özelliklerini kullanmak için lisanslı olarak satın almak gerekir. Örneğin 4 bölümlük bir oyunun sadece 1 bölümünün oynanabilir olması.
4. **Paylaşılan Yazılım (Shareware):** Tanıtım amaçlı hazırlanmış, süre sınırı bulunan yazılımlardır. Örneğin, 30 günlük Office.

## Bilişim Suçları:

Bilgi ve iletişim teknolojilerini kullanarak işlenen tüm suçlara **bilişim suçları** denir.

### En Çok Karşılaşılan Bilişim Suçları:

1. Kredi kartı dolandırıcılığı
2. Sahte hesap açma
3. Başka kişiler/topluluklar hakkında nefret söylemi
4. Sosyal ağlarda sahte hesaplarla hakaret etmek
5. Ücretli oyun ve yazılımların korsan olarak kullanılması

### Bilişim Suçlarına Karşı Alınabilecek Önlemler:

**İnternet Bilgi Destek Hattı:** Alo 141

**İnternet Bilgi İhbar Merkezi(ihbarweb):** <https://www.ihbarweb.org.tr>

## Dijital Ayak İzi

Bilgisayar, tablet, telefon gibi teknolojileri kullandıktan sonra geriye bırakılan izlere dijital ayak izi denir. İnternette yaptığımız hiçbir şey silinmez, arkamızda iz bırakır.



## GİZLİLİK VE GÜVENLİK

### Bilişim Teknolojilerinde Gizlilik ve Güvenlik

Dijital ortamdaki bilgilerimiz okuma-yazma-taşıma esnasında bozulabilir. Depolama araçları (*sabit disk, flash bellek, CD-DVD vb.*) fiziksel hasar görebilir. Yangın, su baskını, deprem gibi felaketler bilgisayarlara zarar verebilir. Virüsler dosyalarımıza zarar verebilir. İstenmeyen kişiler dosyalarımıza erişip işlem yapabilir. Tüm bu durumlar, bilişim teknolojilerinde bilgi güvenliğinde açık oluşturur. Bilgi güvenliği **üç temel unsurdan** oluşur.

- **Gizlilik:** Bilgilerin yetkisiz kişilerin eline geçmemesi ve yetkisi olmayanlara karşı koruyucu önlemler alınmasıdır. Örneğin; bazı internet sitelerinde içerikler sadece üye olanlara görülmektedir.
- **Erişilebilirlik:** Bilginin ihtiyaç duyulduğunda sadece yetkisi olanların kullanabilmesine açık olmasıdır. Örneğin; e-okul sisteminde öğrenciler notlarını sadece görüntüleyebilirken, öğretmenler öğrenci notlarını değiştirebilmektedir.
- **Bütünlük:** Bilgilerin; çeşitli yollarla değiştirilmesinin, silinmesinin engellenmesidir.

## Güvenlik Açıkları ve Bilgi Koruma Yöntemleri

İstemediğimiz kişilerin verilerimize (bilgilerimize) erişmesini engellememiz gerekir. Bilgilerimizin güvenliğini sağlayamazsak bu durumda sistemimizde güvenlik açıkları oluşur. Güvenlik açıkları virüslerin ve bilgisayar korsanlarının verilerimize ulaşmasını kolaylaştırır.

### Bilgi Güvenliğine Yönelik Tehditler

- Bilgilerin donanımsal sebeplerle (okuma-yazma-taşıma sırasında) bozulması.
- Fiziksel zararlar (flash belleği düğürmek, CD-DVD kırmak gibi)
- Zararlı yazılımların etkileri
- Kullanıcısı hatası sonucu kaybolma-silinme

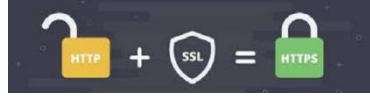
### Bilgi Güvenliğine Yönelik Öneriler

- Güncel bir güvenlik yazılımı kullanın.
- Önemli bilgilerinizi farklı depolama araçlarında (taşınabilir disk, bulut depolama gibi) yedekleyin.
- Dosyalarınızı şifreleyin.
- Genel kullanıma açık yerlerde hesaplarınızın oturumunu kapatın.
- Genel kullanıma açık yerlerde hesaplarınıza **Beni Hatırla** seçeneği ile giriş yapmayın.



Güvenli internet sitesi https ile başlar.

Örnek: <https://www.google.com>



## Zararlı Yazılımlar

Bilgisayara ve bilgilere zarar vermek amacıyla hazırlanmış yazılımlara **zararlı yazılım** denir. Zararlı yazılımlar 5'e ayrılır.

1. **Virüsler:** Bilgisayara izinsiz girip dosya ve programlara zarar verir. Virüsler işletim sistemini bozabilir, dosyalara zarar verebilir ya da silebilir.
2. **Truva Atı(Trojan):** Uygulama gibi çalışır.Bilgisayarda güvenlik açığı oluşturur. Böylece istenmeyen kişiler izinsiz müdahale edebilir.
3. **Solucan (Worm):** Ağ üzerinden bilgisayarımıza bulaşan ve kendini sürekli kopyalayarak çoğaltan zararlı bir yazılımdır. Kendini sürekli çoğalttığı için bilgisayarı yavaşlatır. Gereksiz yer kaplar.
4. **Reklam Yazılımı (Adware):** Herhangi bir program kullanırken ya da internette gezinirken kendiliğinden reklam açan zararlı bir yazılımdır.
5. **Casus Yazılım (Spyware):** Bilgisayardaki bilgileri toplayıp uzaktaki bir kullanıcıyı bilgimiz olmadan gönderen yazılımdır.

## Güvenlik Yazılımları

Zararlı yazılımlardan korunmak amacıyla kullanılan yazılımlardır. Bunlar **antivirüs programları** ve **güvenlik duvarıdır**.

Örnek: Avira, Avast, AVG, Total360 gibi.