ETİK, GÜVENLİK VE TOPLUM

Bilgisayar Bilimi - Kur 1

Ünite - 1

ETİK

NE DEMEK?

Etik

- Bireylerin ahlaklı ve erdemli bir hayat yaşayabilmesi için **hangi davranışlarının doğru, hangilerinin yanlış** olduğunu araştıran bir felsefe dalıdır.
- Temelinde güzel ahlaklı, adaletli ve iyi insan olma vardır.

1.1. Etik Değerler

- Bir konuya ya da belirli bir meslek dalına özgü etik davranışların tamamı **etik değerler** olarak tanımlanabilir.

1.2. Bilişim Etiği

- Bilişim teknolojilerinin ve İnternet'in kullanımı sırasında uyulması gereken kuralları tanımlayan ilkelere **bilişim etiği** denir.

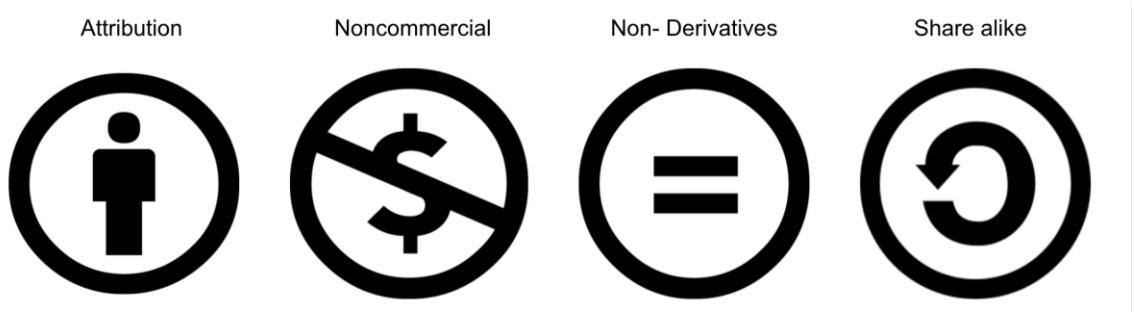
I. Fikri Mülkiyet
II. Erişim
III. Gizlilik
IV. Doğruluk

1.2.1. Fikri Mülkiyet

- Kişinin kendi zihni tarafından ürettiği her türlü ürün sahipliği
- Telif hakkı, patent, şifreleme
- Creative Commons Lisansı (CC)
- GPL Lisans

Creative Commons Lisansı (CC)

- Creative Commons, telif hakları konusunda esneklik sağlamayı amaçlayan, eser sahibinin haklarını koruyarak, eserlerin paylaşımını kolaylaştırıcı modeller sunan, kar amacı gütmeyen bir organizasyondur.

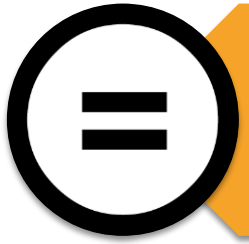


Atıf (Attribution)

- Eserin ilk sahibinin belirtilmesi koşulu

Ticari Olmayan (Non-Commercial)

- Eserin ticari amaçlı kullanılmaması koşulu



Türetilemez (No Derivate Works)

- Eserin türevinin yapılmaması koşulu

Aynı Lisansla Paylaş (Share Alike)

- Yapılacak yeni eserin de aynı lisansa sahip olması koşulu

GPL Lisansı

- General Public Licence / Genel Kamu Lisansı
- Programı sınırsız kullanma özgürlüğü.
- Programın nasıl çalıştığını inceleme ve amaçlara uygun değiştirme özgürlüğü.
- Programın kopyalarını sınırsız dağıtma özgürlüğü.
- Programın değiştirilmiş halini dağıtma özgürlüğü.

1.2.2. Erişim

- Sıradan bir vatandaş için herhangi bir bilişim teknolojisi ürününden bilgiye erişebilmesi olarak düşünülebilir.
  - Bilgiye erişebilecek düzeyde bilişim bilgisi
  - Bilginin yararlılığını test edecek düzeyde bilgi okuryazarlığı
  - Bilgiye erişmenin varsa maddi karşılığı olan ekonomik güç

1.2.3. Gizlilik

- Kişiye ait her türlü bilgiyi (ki bu bilgi sadece ad ve soyadı değil, kişinin duygu, düşünce, siyasi eğilim, dini inancı, planı, fantezi dünyası ve korku gibi bilgilerini de içerir) saklama becerisidir.

Google

DuckDuckGo


Be vigilant
MUTLAKA SONUNA
KADAR İZLEYİN...

1.2.4. Doğruluk

- Sorumluluk kimde?
- Her bilgi doğru mu? Kaynak belirtilmiş mi?
- En az üç kaynaktan kontrol!
- Adres kontrol edilmeli.

- **com** → ticari şirketler (commercial)
- **org** → dernek, sendika gibi sivil toplum örgütleri (organization)
- **gov** → devlete ait siteler (government)
- **edu** → üniversiteler (education)
- **k12** → 12 yıllık eğitime dahil ilkokul, ortaokul ve liseler
- **net** → internet, ağ üzerine iş yapan şirketler (network)
- …

e okul

Tümü | Haberler | Videolar | Görseller | Alışveriş | Daha fazla | Ayarlar | Araçlar

Yaklaşık 3.320.000 sonuç bulundu (0,24 saniye)

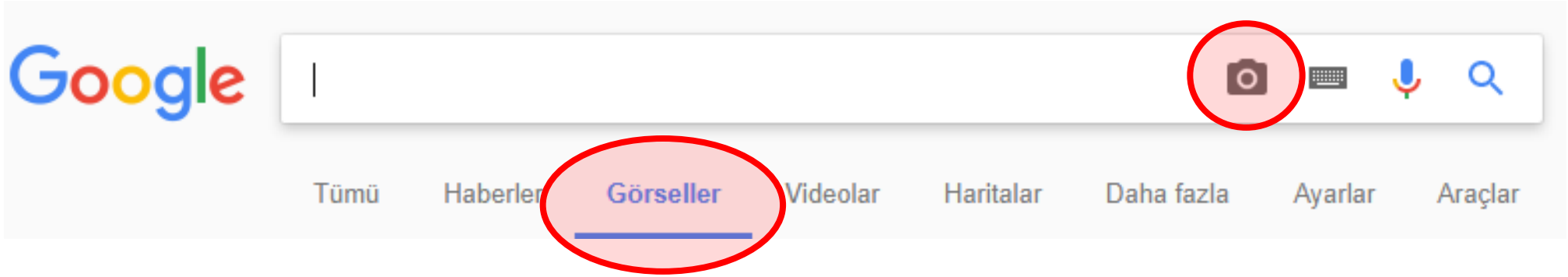
E-Okul Veli Bilgilendirme Sistemi - Meb
https://e-okul.meb.gov.tr/

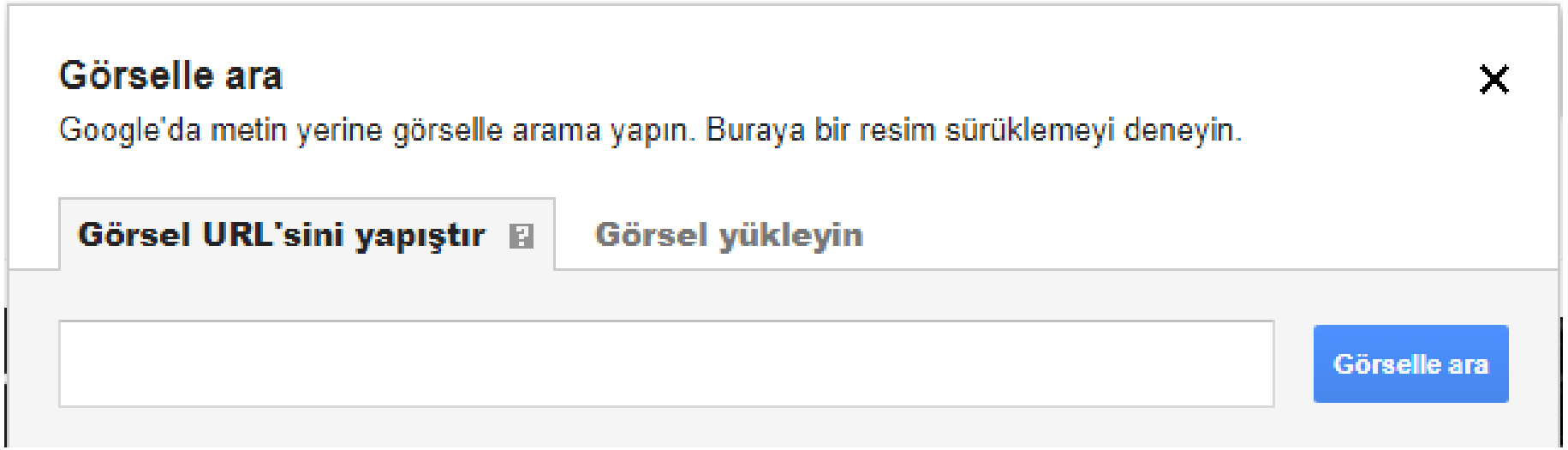
T.C. Millî Eğitim Bakanlığı e-Okul Yönetim Bilgi Sistemi
https://eokulyd.meb.gov.tr/
2017-2018 öğretim yılı e-Kayıt uygulaması sonucu adres bilginize göre Anasınıfı, İlkokul 1. sınıf veya Ortaokul 5. sınıfa kayıt yaptırmanız gereken okulu görmek ...

e-Okul İlkÖğretim Uygulamaları
https://eokulyd.meb.gov.tr/IlkOgretim/MEM/IOM00009.aspx
2017-2018 Öğretim Yılı **Okul** Öncesi - İlkokul - Ortaokul e-Kayıt Sonuçları. Giriş Kodunuz, : Giriş Kodu, : T.C. Kimlik No, : Doğum Tarihi, : GG/AA/YYYY ...

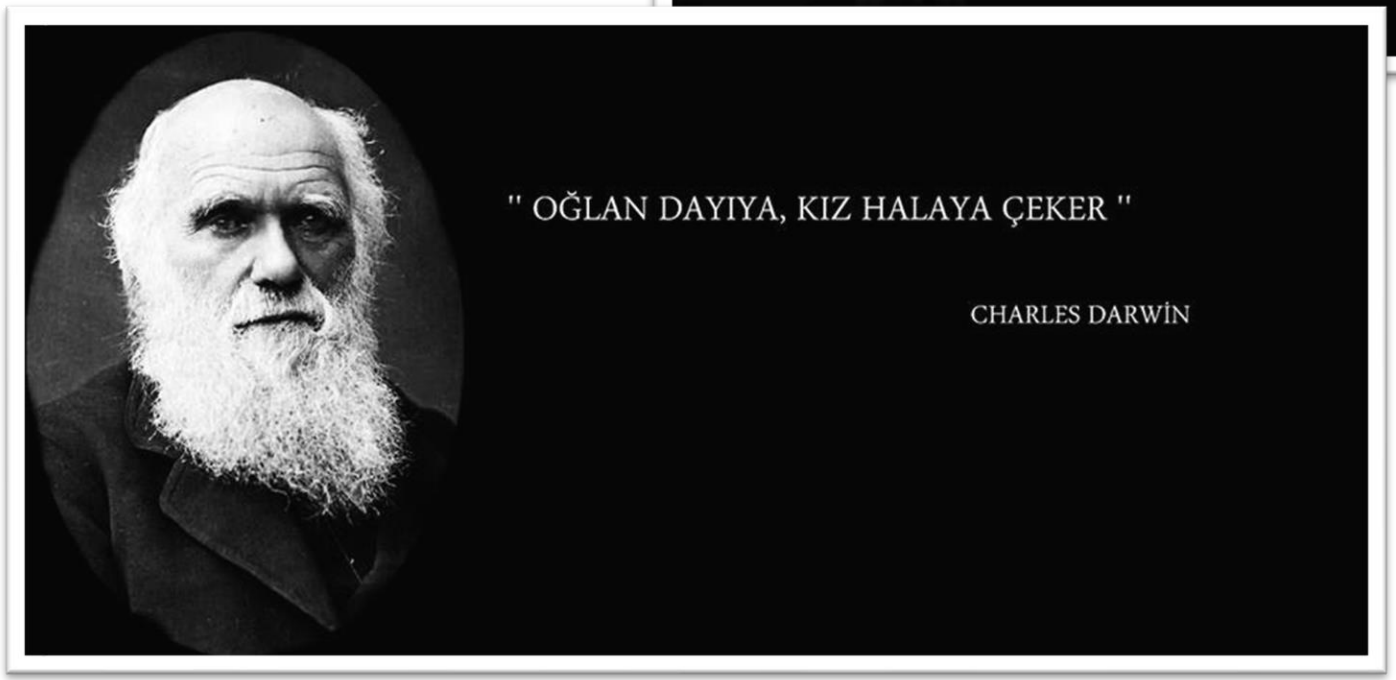
e-Okul Veli Bilgilendirme Sistemi
www.eokul-meb.com/
e **okul** Veli bilgilendirme sistemi, TEOG Sonuçları 2017 e **okul** öğrenci haber e **okul** yönetim bilgi sistemi giriş Öğrenci ve öğretmen meb **eokul** vbs.

MEB e-okul


Google
Tümü
Haberler
Görseller
Videolar
Haritalar
Daha fazla
Ayarlar
Araçlar


Görselle ara
Google'da metin yerine görselle arama yapın. Buraya bir resim sürüklemeyi deneyin.
Görsel URL'sini yapıştır
Görsel yükleyin
Görselle ara


Üst üste geliyorsa dertler,
CTRL+ALT+DEL yap geçer...
- Bill Gates


" OĞLAN DAYIYA, KIZ HALAYA ÇEKER "
CHARLES DARWİN

teyit.org

1.2.5. İnternet Etiği

- Bize yapılmasından hoşlanmadığımız davranışları başkalarına yapmaktan kaçınmalıyız
- İnternet'i kullanırken her kültüre ve inanca saygılı olmalıyız
- Sürekli büyük harfler ile yazışmanın yüksek sesle konuşmak anlamına geldiği unutulmamalı.
- Kaba, argo konuşmamalıyız.

1.2.5. İnternet Etiği

- Özel hayatlara saygı gösterilmeli, kişilere ait sırlar paylaşılmamalıyız.
- İzinsiz bilgi paylaşımı yapmamalıyız.
- Doğruluğundan emin olmadığımız bilgi, belge veya haberi doğruymuş gibi paylaşmamalıyız.
- İnterneti başkalarına zarar vermek amaçlı kullanmamalıyız.


Internet Society
Turkey Chapter
İnternet Derneği
ISOC-TR

Siber (Dijital) Zorbalık

- Zorbalık yapan hesaplara cevap vermeyin, tartışmaya girmeyin, hesabı engelleyin ve bu hesapları **“Bildir/Şikâyet Et”** bağlantısını kullanarak şikâyet edin.
- Size yönelik etik dışı davranışlara ait ekran görüntülerini veya mesajları kaydedin ve hukuki yollara başvurun.

1.3. Bilgi Güvenliği

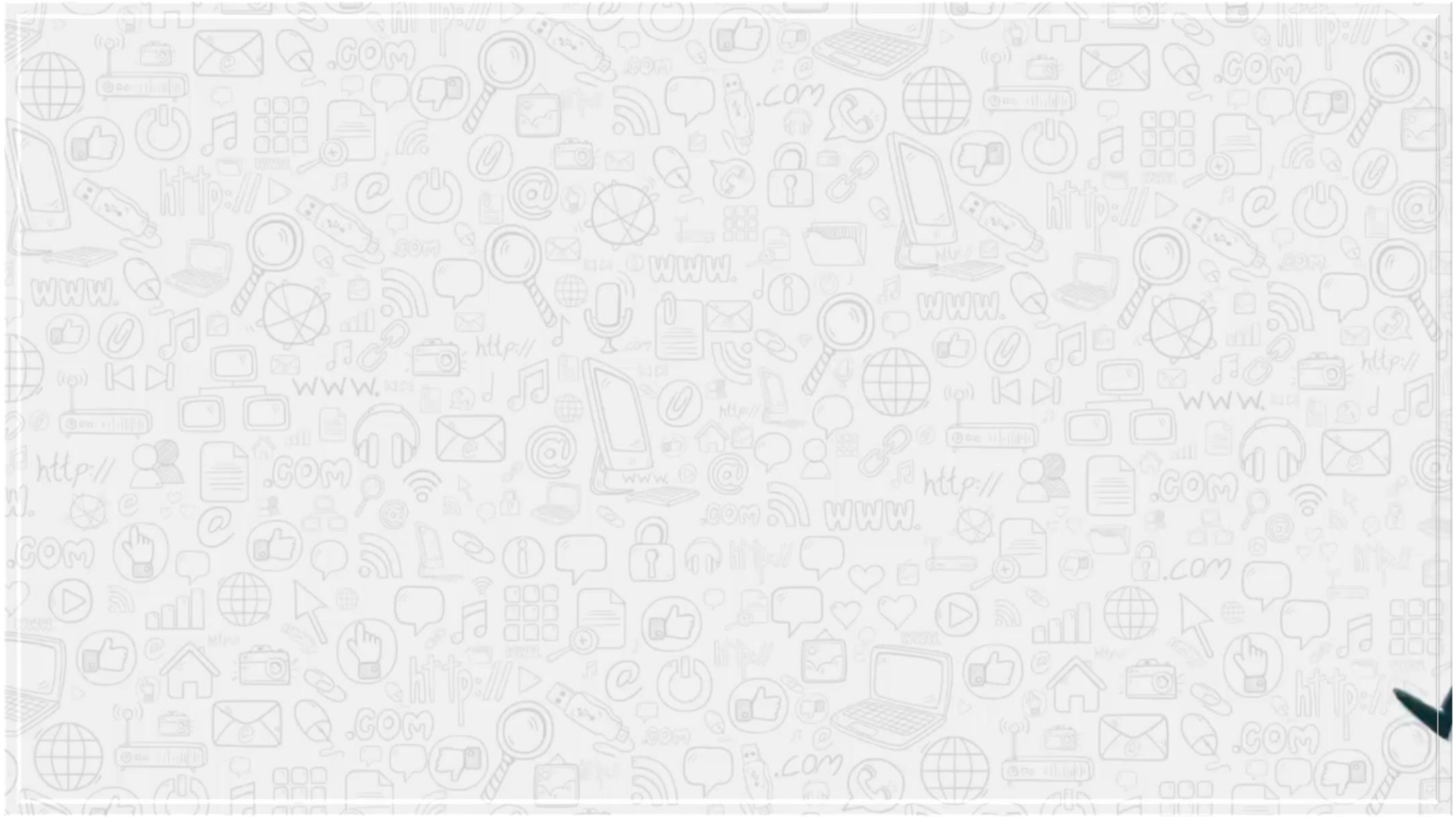
- Önem teşkil eden her tür bilgiye izin alınmadan ya da yetki verilmeden erişilmesi, bilginin ifşa edilmesi, kullanımı, değiştirilmesi, yok edilmesi gibi tehditlere karşı alınan tüm tedbirlere bilgi güvenliği denir.
  - Gizlilik
  - Bütünlük
  - Erişilebilirlik

1.3.1. Bilgi Güvenliğine Yönelik Tehditler

- **Siber:** Temeli bilişim teknolojilerine dayanan, tüm cihaz ve sistemleri kapsayan yapıya verilen genel addır
- **Siber Suç:** Bilişim teknolojileri kullanılarak gerçekleştirilen her tür yasa dışı işlemdir.
- **Siber Saldırı:** Hedef seçilen şahıs, şirket, kurum, örgüt gibi yapıların bilgi sistemlerine veya iletişim altyapılarına yapılan planlı ve koordineli saldırıdır.

1.3.1. Bilgi Güvenliğine Yönelik Tehditler

- **Siber Savaş:** Farklı bir ülkenin bilgi sistemlerine yapılan planlı ve koordineli saldırılardır.
- **Siber Terörizm:** Bilişim teknolojilerinin belirli bir politik amaca ulaşabilmek için hükümetleri, toplumu, bireyleri ve kuruluşları yıldırma, baskı altında tutma amacıyla kullanılmasıdır.
- **Siber Zorbalık:** Bilgi ve iletişim teknolojilerini kullanarak bir birey ya da gruba, özel ya da tüzel bir kişiliğe zarar verme davranışlarının tümüdür.



1.3.2. Sayısal Dünyada Kimlik ve Parola Yönetimi

- Parola, **büyük/küçük harfler, noktalama işaretleri ve özel karakterler** içermelidir.
- Parola, -aksi belirtilmedikçe- **en az sekiz karakter** uzunluğunda olmalıdır.
- Parola, **ardışık harfler ya da sayılar içermemelidir.**
- **Belirli aralıklar ile yeni parola** oluşturulması gerekir.
- Parola başkalarıyla **paylaşılmamalıdır**.

1.3.2. Sayısal Dünyada Kimlik ve Parola Yönetimi

- Parolalar, basılı ya da elektronik olarak hiçbir yerde **saklanmamalıdır**.
- Başta e-posta adresinin parolası olmak üzere farklı bilişim sistemleri ve hizmetler için **aynı parolanın kullanılmaması** gerekir.

Diğer Güvenli Parola Oluşturma İpuçları

- Basit bir kelimenin içindeki harf, rakam ve sembolleri **birbirine benzeterek** değiştirebilirsiniz. **Örneğin; B yerine 8, 3 yerine E, a yerine @...**

- Mevcut parolanızı daha da güçlendirmek için parolanıza kullandığınız siteye özel harf, rakam ve semboller ekleyebilirsiniz. **Örneğin; parolanız "*Vy1LD1z*" olsun, mail şifreniz "*Vy1LD1z+m@il*", sosyal medyaya ait parolanız "*Vy1LD1z+*FB" olabilir.**

1.3.3. Kişisel Bilgisayarlarda ve Ağ Ortamında Bilgi Güvenliği

Zararlı yazılımlar

- İşletim sisteminin ya da diğer programların çalışmasına engel olabilir, sistemdeki dosyaları silebilir, değiştirebilir ya da yeni dosyalar ekleyebilir.
- Bilişim sisteminde bulunan verilerin ele geçirilmesine neden olabilir.
- Güvenlik açıkları oluşturabilir.
- Başka bilişim sistemlerine saldırı amacıyla kullanılabilir.
- Bilişim sisteminin, sahibinin izni dışında kullanımına neden olabilir.
- Sistem kaynaklarının izinsiz kullanımına neden olabilir.

1.3.3. Kişisel Bilgisayarlarda ve Ağ Ortamında Bilgi Güvenliği

- Zararlı Yazılımlar; Bilişim sistemlerinin çalışmasını bozan veya sistem içinden bilgi çalmayı amaçlayan kötü niyetlerle hazırlanmış yazılımlardır.
- Virüs Çeşitleri;
  - Solucan (worm)
  - Truva Atı (Trojan)
  - Casus (Spyware)
  - Keylogger

Zararlı Programlara Karşı Alınacak Tedbirler

- Bilgisayara **antivirüs ve İnternet güvenlik programları** kurularak bu programların **sürekli güncel** tutulmaları sağlanmalıdır.

- **Tanınmayan/güvenilmeyen e-postalar ve ekleri** kesinlikle açılmamalıdır. Örneğin resim.jpg.exe isimli dosya bir resim dosyası gibi görünse de uzantısı exe olduğu için uygulama dosyasıdır.

Zararlı Programlara Karşı Alınacak Tedbirler

- Zararlı içerik barındıran ya da tanınmayan web sitelerinden uzak durulmalıdır.
- **Lisanssız ya da kırılmış programlar** kullanılmamalıdır.
- Güvenilmeyen İnternet kaynaklarından dosya indirilmemelidir.

Kaynaklar

- Sunu hazırlanırken Bilgisayar Bilimi Kur 1 Kitabından yararlanılmıştır.