

1. Etik Deęerler

- Bireylerin ahlaklı ve erdemli bir hayat yaşayabilmesi için hangi davranışlarının doğru, hangilerinin yanlış olduğunu araştıran bir felsefe dalı
- Temelinde güzel ahlaklı, adaletli ve iyi insan olma
- Bir konuya ya da belirli bir meslek dalına özgü etik davranışların tamamı **etik deęerler** olarak tanımlanabilir.
- Bilişim teknolojilerinin ve İnternet'in kullanımı sırasında uyulması gereken kuralları tanımlayan ilkelere **bilişim etięi** denir.

Fikri Mülkiyet

- Kişinin kendi zihni tarafından ürettiği her türlü ürün sahipliği
- Fikirler, şarkı sözleri, şiir, resim, fotoğraf, yazılımlar
- Eserlerin (bilişim alanı için geliştirilen yazılımlar) sahibi kimdir ve kimlerin kullanımına izin verilmiştir?
- <https://ggm.gtb.gov.tr/sikca-sorulan-sorular/ticari/fikri-mulkiyet-haklari>

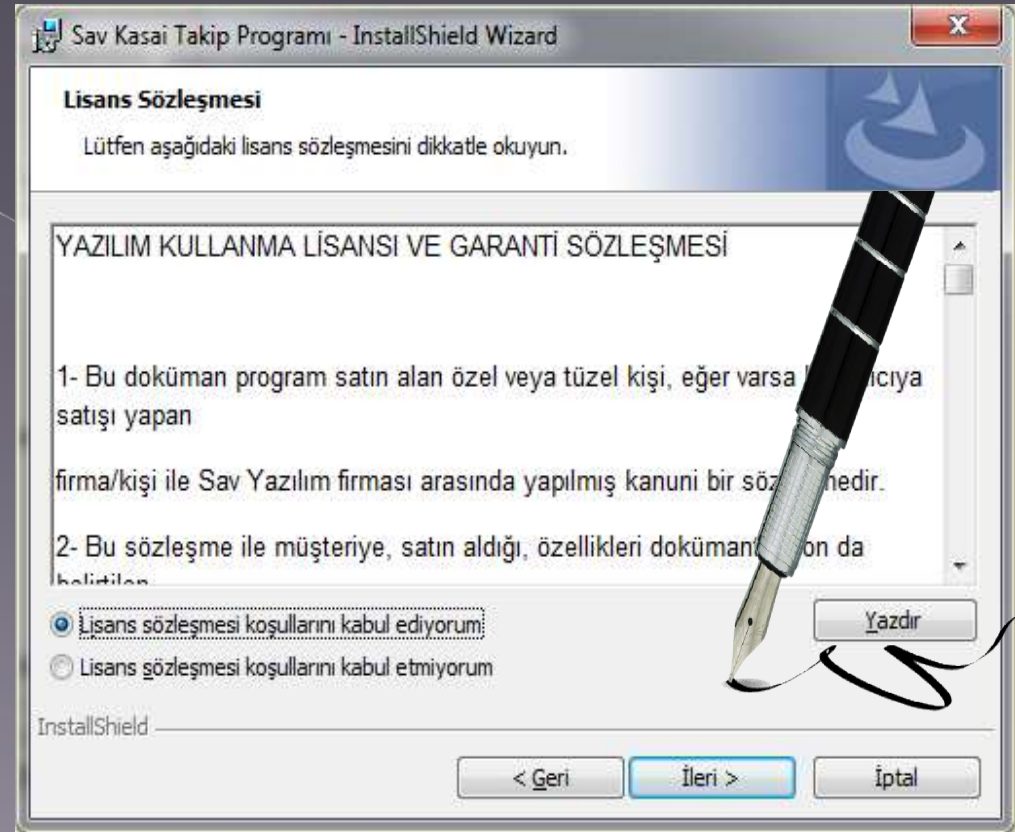


Telif Hakkı

- Fikir sanat ürününün satılması, çoğaltılması, dağıtılması, paylaşılması gibi tüm hakları içerir.

Lisans : Fikir sanat ürününün, yazılımın kullanılmasında kullanıcının haklarının ve sınırlarının belirlendiği sözleşmedir.

- Lisanslama işlemlerinde iki organizasyon öne çıkmaktadır.
- ❖ CC(creative commons)
- ❖ GPL(General public 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.
- Bu organizasyona dahil olan eserler, kaynağı belirtmek on şartıyla belirli kısıtlamalar göz önünde bulundurularak kullanılabilir.

Koşullar

Creative Commons (CC)



Attribution - Atıf: Eserin ilk sahibinin belirtilmesi koşulu. Bu koşulu barındıran lisansa sahip eserlerde, eseri yaratan ilk kişinin mutlaka belirtilmesi gerekiyor.



Share Alike - Aynı Lisansla Paylaş: Lisans modelinin korunması koşulu. Bu koşula sahip eserlerin türetilmesi veya yeniden yayınlanması ancak onu barındıran yeni eserin de aynı lisansa sahip olması şartıyla gerçekleşebilir.



Non-Commercial - Ticari Olmayan: Eserin ticari amaçlı kullanılmaması koşulu. Bu koşulu şart koşan eserlerin türevlerinin veya orijinallerinin sadece ticari olmayan ürünlerde kullanılması mümkün (Ticari amaçlı kullanmak için eser sahibine başvurmak mümkün.).



No Derivate Works - Türetilemez: Eserin türevinin yaratılmaması koşulu. Bu koşulu içeren lisanslı eserlerin türevlerinin yapılmasına izin verilmemektedir eğer isteniyorsa sadece olduğu gibi kullanılması gerekir.

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.

Diđer Yazılımlar

- ◉ Ücretsiz Sürümler
 - > Freeware
- ◉ Deneme Sürümleri
 - > Shareware / Demo
 - > Zaman veya özellik kısıtlı
- ◉ Paralı sürümler
 - > Full

Not: Tüm yazılımlarda lisans sözleşmesi olabilir.

Eriřim (Bilgiye Eriřim)



Bilgiye eriřebilecek düzeyde biliřim bilgisi,

Bilginin yararlılıđını test edecek düzeyde bilgi okuryazarlıđı,

Bilgiye eriřmenin varsa maddi karřılıđı olan ekonomik g¼ç.

Herhangi bir biliřim teknolojisi ¼r¼n¼nden bilgiye eriřimde kiřinin tařıması gereken ¼zellikler



2.3. Gizlilik

- Kişiyeye ait her türlü bilgiyi saklama becerisi,
- **Gizlilik:** Bilginin yetkisiz kişilerce görülmesinin engellenmesidir.



Zuckerberg'in Fotoğrafında dikkat çeken ayrıntı!
**LAPTOP'UN KAMERASI NEDEN BANTLI?
DİNLENME VE İZLENME ENDİŞESİMİ!**

GADGET
2023

Google

2.4. Doğruluk

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



Uluslararası Bilgisayar Etik Enstitüsüne göre bilişim teknolojilerinin doğru bir şekilde kullanılabilmesi için aşağıda belirtilen 10 kurala uyulması gerekmektedir.

- 1. Bilişim teknolojilerini başkalarına zarar vermek için kullanmamalısınız.
- 2. Başkalarının bilişim teknolojisi aracılığı ile oluşturduğu çalışmalarını karıştırmamalısınız.
- 3. Başkasına ait olan verileri incelememelisiniz.
- 4. Bilişim teknolojilerini hırsızlık yapmak için kullanmamalısınız.
- 5. Bilişim teknolojilerini yalancı şahitlik yapmak için kullanmamalısınız.
- 6. Lisanssız ya da kırılmış/kopyalanmış yazılımları kullanmamalısınız.
- 7. Başkalarının bilişim teknolojilerini izinsiz kullanmamalısınız.
- 8. Başkalarının bilişim teknolojileri aracılığı ile elde ettiği çalışmalarını kendinize mal etmemelisiniz.
- 9. Yazdığınız programların ya da tasarladığınız sistemlerin sonuçlarını göz önünde bulundurmalısınız.
- 10. Bilişim teknolojilerini her zaman saygı kuralları çerçevesinde kullanmalı ve diğer insanlara saygı duymalısınız.

meb.gov.tr

Kurum/Kuruluş/Şirket

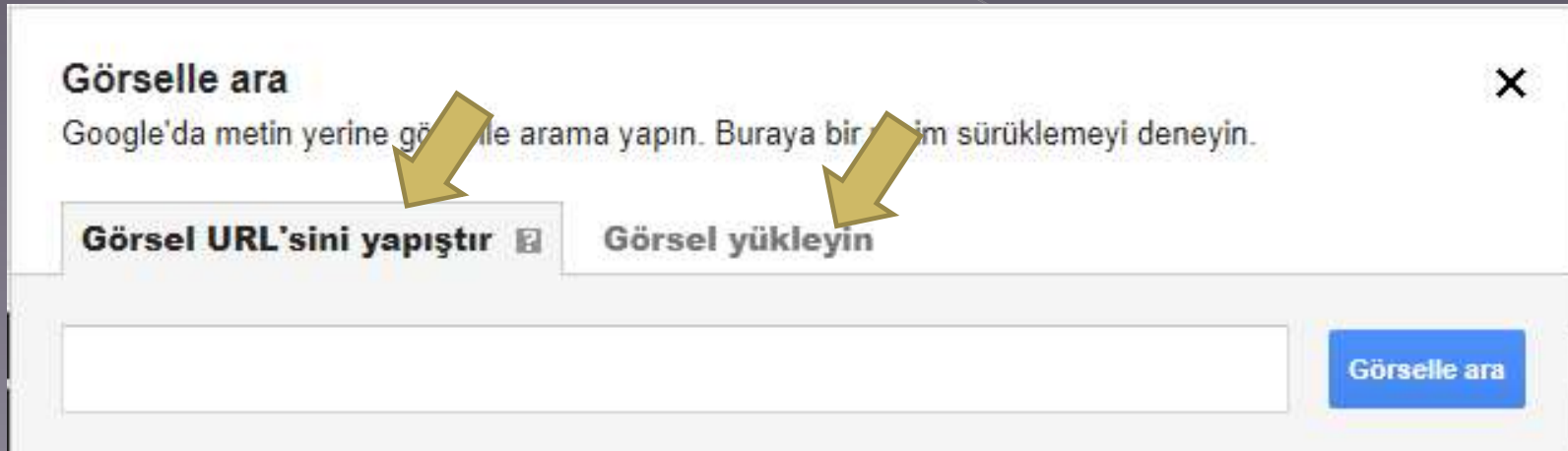
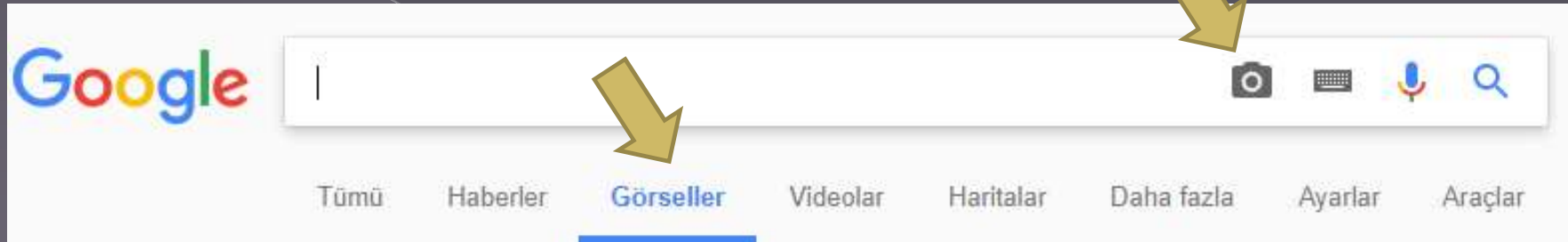
Kategori Uzantısı

Ülke Kodu

- 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 olan okullar /ilkokul, ortaokul ve liseler
- net → internet, ağ üzerine iş yapan şirketler /network
- ...

SY Suriye
SZ Svaziland
TC Turks ve Caicos Adası
TD Çad
TF Fransız Güney Toprakları
TG Togo
TH Tayland
TJ Tacikistan
TK Tokelau
TM Türkmenistan
TN Tunus
TO Tonga
TP Doğu Timor
TR TÜRKİYE
TT Trinidad ve Tobago
TV Tuvalu
TW Tayvan
TZ Tanzanya
UA Ukrayna
UG Uganda
UK Birleşik Krallık
UM US Minor Outlying Adası
US Amerika Birleşik Devletleri
UY Uruguay
UZ Özbekistan

Benzer Görseli Arayın



2.5. İnternet Etiđi

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

BİLGİ GÜVENLİĞİ

- 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**: Bilginin yetkisiz kişilerce görülmesinin engellenmesidir.
- ◉ **Bütünlük**: Bilginin yetkisiz kişiler tarafından değiştirilmesi ya da silinmesi gibi tehditlere karşı korunmasıdır.
- ◉ **Erişilebilirlik**: Bilginin yetkili kişilerce ihtiyaç duyulduğunda ulaşılabilir ve kullanıma hazır durumda olmasıdır.

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.
- **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.

Siber (Dijital) Zorbalık

- Zorbalık yapan hesaplara;
 - > cevap vermeyin,
 - > tartışmaya girmeyin,
 - > hesabı engelleyin.
- Bu hesapları, bulunduğunuz sosyal medya platformundaki “Bildir/Şikâyet Et” bağlantısını kullanarak şikâyet ediniz.
- Size yönelik etik dışı davranışlar artarak ve ağırlaşarak devam ederse bunların ekran görüntülerini ve mesajları kaydediniz ve hukuki yollara başvurunuz.
- Zorba bir hesap için kötü kullanım bildirim sayısı fazla olursa o hesabın site yönetimi tarafından incelenmesi ve kapatılması daha çabuk olacaktır.



Parola ? Şifre ? Pin ?

- “parola” bir hizmete erişebilmek için gerekli olan, kullanıcıya özel karakter dizisidir.
- “Şifre” sanal ortamdaki verilerin gizliliğini sağlamak için veriyi belirli bir algoritma kullanarak dönüştüren yapıdır.
- “Pin” 1234567890

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.
- 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.



Güvenli Parola Oluşturma Yöntemleri

- Anahtar kelime oluştururken; G yerine 6, g yerine 9, Ş yerine \$, a yerine @, i veya l yerine 1 gibi karakterler kullanılabilir.
- Alsancak → A1s@nc@k → Twitter için A1s@nc@k TW gibi..
- “Muhtaç olduğun kudret, damarlarındaki asil kanda mevcuttur.” → M0kd@kM@il (e-posta için)

Kişisel Bilgisayarlarda ve Ağ Ortamında Bilgi Güvenliği

Virus (Virüs) : Bilgisayar, dizüstü, tablet, akıllı telefon, akıllı televizyon, ip/bebek kamera, güvenlik sistemi cihazları ana üniteleri dahil yazılımsal olarak bir işletim sistemi bulunan tüm cihazlarda, komple yazılım veya bitişik kod bloğu olarak barınabilen zararlı faaliyetlere hizmet eden tüm program yapılarına verilen genel isimlendirme.

Zararlı Yazılım (Malware): Bilişim sistemlerinin çalışmasını bozan veya sistem içinden bilgi çalmayı amaçlayan kötü niyetlerle hazırlanmış yazılımlardır.

- Solucan (worm): Kendiliğinden çalışır ve kendi kendini kopyalar.
- Truva Atı (trojan): Görünürde masum bir yazılım, arka planda veri çalar.
- Casus (spyware): İstatistiki bilgi toplar. Genelde interneti yavaşlatır.
- Keylogger(tuş kaydedici): klavyede basılan her tuşu kaydedip sahibine gönderir



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 içerik barındıran ya da tanınmayan web sitelerinden uzak durulmalıdır.
- Lisanssız ya da kırılmış programlar kullanılmamalıdır.
- Güvenilmeyen İnternet kaynaklarından dosya indirilmemelidir.
- Bilgisayarınızda dosyaların uzantıları sürekli görünür şekilde listelenmelidir



Dosya Uzantısı: Bir Windows dosya isminin içindeki en son noktadan itibaren dosya sonuna kadar olan ve genelde üç harften oluşan bölümdür.

- ⦿ Kendi başına çalışan ve virüs içerebilen dosya türlerine örnek olarak ***.exe, *.com, *.vbs, *.js, *.scr, *.msi *.bat** dosyalarını gösterebiliriz. ("*" işareti dosya ismini temsil etmektedir.)
- ⦿ Kesinlikle virüs içermeyen dosya türlerine örnek olarak ses dosyaları (*.mp3, *.wav, *.mid), metin dosyaları (*.txt, *.pdf, *.ini, *.log), resim dosyaları (*.bmp, *.jpg, *.gif, *.ico), film dosyaları (*.mpg, *.mpeg, *.avi, *.asf) örnek olarak gösterilebilir.
- ⦿ Word (*.doc) ve Excel (*.xls) dosyaları makro virüsü içerebilir. Eğer bir *.doc dosyasında makro varsa Word (veya Excel) açılışta makroyu etkinleştirip etkinleştirmeyeceğinizi size soracaktır. Bir Word dosyasının makro içermesi mutlaka virüs içerdiği anlamına gelmez.