ETİK,GÜVENLİK VE TOPLUM

Etik değerler

Etik; bireylerin ahlaklı ve erdemli bir hayat yaşayabilmesi için hangi davranışlarının doğru, hangilerinin yanlış olduğunu araştıran bir felsefe dalıdır.

- Temelinde barındırdığı güzel ahlaklı, adaletli ve iyi insan olma özellikleri değişmese de zamana, bilimsel gelişmelere ve toplumun gereklerine göre etik kavramına yüklenen anlam değişebilmektedir.

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

- Etik dışı eylemlere ilişkin yaptırımlar, çoğu zaman toplum tarafından belirlenmekte ve bu yaptırımlar gerekirse yasal düzenlemeler için belirleyici olmaktadır.

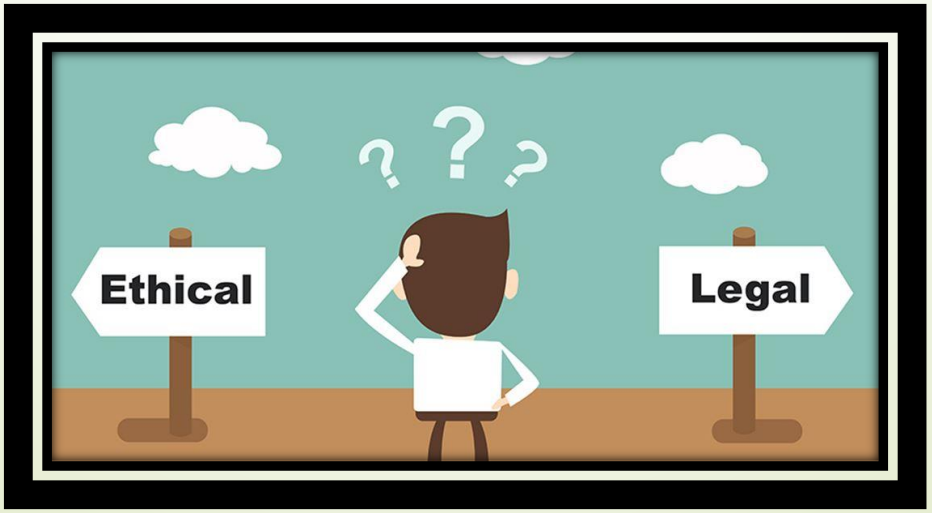
- Bilişim teknolojilerinde yaşanan hızlı değişim ve yaygınlaşma, istenen bilgiye her zaman ve her yerde erişebilme imkânı gibi faydalar sunmasının yanı sıra bu teknolojilerin tam olarak anlaşılmadan kullanımına yol açmakta ve bu durum da beraberinde pek çok sorun ortaya çıkarmaktadır.

- Bu anlamda yaşanan sorunlardan birisi de zaman ve mekân sınırı olmaksızın erişilen bilginin doğruluğunun ve kaynağının tespitidir.

- Gelişmiş toplumun önemli göstergelerinden birisi de gerek üretilen bilginin gerekse bu bilgiyi kullanan bireylerin etik kurallara uyup uymadıklarıdır.

Bilişim Teknolojileri ve İnternet Kullanımında Dikkat Edilmesi Gereken Etik İlkeler

- Bilişim teknolojilerinin ve İnternet'in kullanımı sırasında uyulması gereken kuralları tanımlayan ilkelere **bilişim etiği** denir.
- Bu ilkelerin temel amacı, bilişim teknolojileri ve İnternet'i kullanan bireylerin yanlış bir davranış sergilemesine engel olarak onları güvence altına almaktır. Bilişim teknolojilerinin kullanımında yaşanan etik sorunların dört temel başlıkta (fikrî mülkiyet, erişim, gizlilik ve doğruluk) ele alındığı görülmektedir.



Fikrî Mülkiyet

- Fikrî mülkiyet; kişinin kendi zihni tarafından ürettiği her türlü ürün olarak tanımlanmaktadır.
  Türk Dil Kurumu ise Bilim ve Sanat Terimleri Sözlüğü'nde fikrî mülkiyet kavramını "düşünü çalışması sonunda ortaya konulan yazın ve bilim ürünleri üzerindeki iyelik" olarak tanımlamıştır.

- "Eserlerin (bilişim alanı için geliştirilen yazılımlar) sahibi kimdir ve kimlerin kullanımına izin verilmiştir?" sorularının cevabı fikrî mülkiyet başlığının altında irdelenmektedir.

- Fikrî mülkiyet denince karşımıza hukuki ve etik boyutlar çıkmaktadır. Kimi sorunlar yasal olup etik olmazken kimi de etik olup yasal olmayabilmekte ya da iki boyut birden temelsiz kalabilmektedir.

- Bu nedenle fikrî mülkiyete ilişkin yasalar, günümüz koşullarına uygun olarak güncellenmeye muhtaç olmaktadır. Telif hakkı, patent, şifreleme gibi kavramlar da bu gereksinim sonucunda ortaya çıkmıştır.

Creative Commons Nedir?

- Telif hakları konusunda esneklik sağlamayı amaçlayan, eser sahibinin haklarını koruyarak,
eserlerin paylaşımını kolaylaştırıcı modeller sunan, kâr amacı gütmeyen bir organizasyondur. Bu organizasyona dâhil olan eserler, kaynağı belirtmek ön şartıyla belirli kısıtlamalar göz önünde bulundurularak kullanılabilir.

  CC lisanslı eserler bu kısıtlamaların yalnızca birine sahip olabileceği gibi birden fazlasına aynı anda sahip olabilir. Bu eserlerin kısıtlamaları, eserin bulunduğu sayfanın alt kısmında görülebilir.

Koşullar

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.

YAZILIM ÇEŞİTLERİ

- Bilişim dünyasında yazılımları lisanslarına göre, özgür yazılımlar ve ticari yazılımlar olmak üzere ikiye ayırabiliriz.
- Özgür yazılım dünyasına ait GPL'ye (General Public Licence - Genel Kamu Lisansı) sahip yazılımlar ücretsiz olarak (ya da özelleştirilmiş versiyonları düşük ücretlerle) kullanılabilirken ticari faaliyet gösteren firmaların ürettiği yazılımların lisanslarıysa çoğunlukla yüksek bedeller karşılığında alınabilmektedir.
- Lisanssız yazılım kullanmanın etik uygunsuzluk yanında teknik sakıncaları da vardır. Firmalarca sunulan yazılımlar, zaman zaman güvenlik açıklarını kapatmak ya da ek özelliklerle donanmak amacıyla güncelleme alır. Lisanssız kullanılan yazılımlar, bu güncellemeleri alamaz ve bilgi güvenliği açısından bilgisayarları savunmasız kılar.

Diğer Yazılımlar

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

Not: Tüm yazılımlarda lisans sözleşmesi olabilir.

Erişim

- Herhangi bir arama sitesini kullanarak, istediğimiz bilgiye hızlıca erişebiliriz. Ancak bilgi daha özel bir formatta sunulmuş olabilir. Örneğin bir veri tabanında saklanıyor olabilir. Bu durumda karşımıza üç sorun çıkmaktadır:

  1. Bilgiye erişebilecek düzeyde bilişim bilgisi,
  2. Bilginin yararlılığını test edecek düzeyde bilgi okuryazarlığı,
  3. Bilgiye erişmenin varsa maddi karşılığı olan ekonomik güç.

- Günümüz insanı birinci sorunu aşmakta başarılı gibi görünürken, ikinci sorunda hâlâ güçlükler söz konusudur. Çünkü bilgi yığınları artmakta ve bu bilginin doğruluğunu test etmek güçleşmekte ayrıca son kullanıcı dediğimiz vatandaşın bunu test etme bilincinin eğitilmesi gerekmektedir.
- Üçüncü sorun olan ekonomik boyut için kütüphane veri tabanları bir çözüm olarak karşımıza çıkmaktadır. Bu durumda bilginin ücretsiz olması "Herkesin eşit derecede bilgiden yararlanmasını sağlar." çözüm önerisi, fikrî mülkiyet ile çelişecektir.

Gizlilik

- Google'da arama yaparken karşınıza çıkan reklamların, sizin daha önce ziyaret ettiğiniz siteler ve bunların içeriklerinden elde edilen verilerle tespit edilen ilgi alanlarınıza yönelik olduğunu görmüşsünüzdür.
- Gizlilik dediğimiz kavram 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.
- Ancak bilginin saklanması dışında bu bilginin doğru kişilerle doğru zaman diliminde de paylaşılması gizlilik başlığını ilgilendirir. Örneğin hasta, bilgilerini doktoru ile paylaşmak zorundadır.
- İzlenmekten kaçınmak için açık kaynak dünyasından alternatifler kullanılabilir.
  Örnek olarak https://duckduckgo.com sitesini inceleyiniz.

Video -1 her şeyi bilen adam

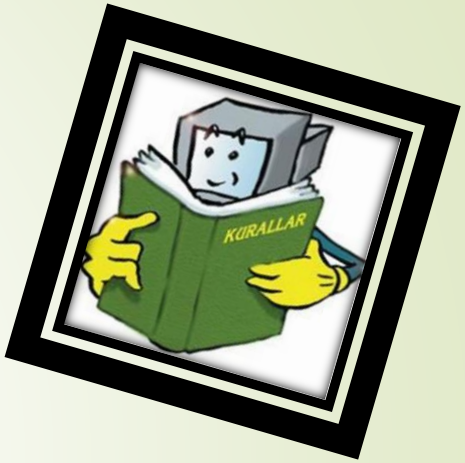
Doğruluk

- Bilgi paylaşım siteleri (wiki ortamları) açık sistemlerdir. Bu sistemlerdeki verilerin doğruluğunun garantisi kimdedir gibi sorular bu başlık altında ele alınmaktadır.

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

Bilişim teknolojilerinin doğru bir şekilde kullanılabilmesi 10 kurala bağlıdır;

1. Bilişim teknolojilerini başkalarına zarar vermek için kullanmamalısınız.



2. Başkalarının bilişim teknolojisi aracılığı ile oluşturduğu çalışmaları 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.

BİLGİYİ DOĞRULAMA KURALLARI

Kullanıcıya bilgi aktaran kanal (İnternet sitesi, sosyal medya hesabı), kaynak belirtmelidir. Kaynağı belirtilmemiş bilgiye şüpheyle yaklaşılmalıdır.

- Elde edilen bilgiler üç farklı kaynaktan teyit edilmelidir.
- Bilgiyi aktaran İnternet sitesinin adresi kontrol edilmelidir.

Alan adı uzantıları birçok İnternet sitesi için fikir verebilir. Örneğin;

.com ya da .net alan adı uzantısına sahip İnternet siteleri ticari amaçlı sitelerdir.

.gov: Devlet kurumlarının resmî sitelerinin uzantısıdır.

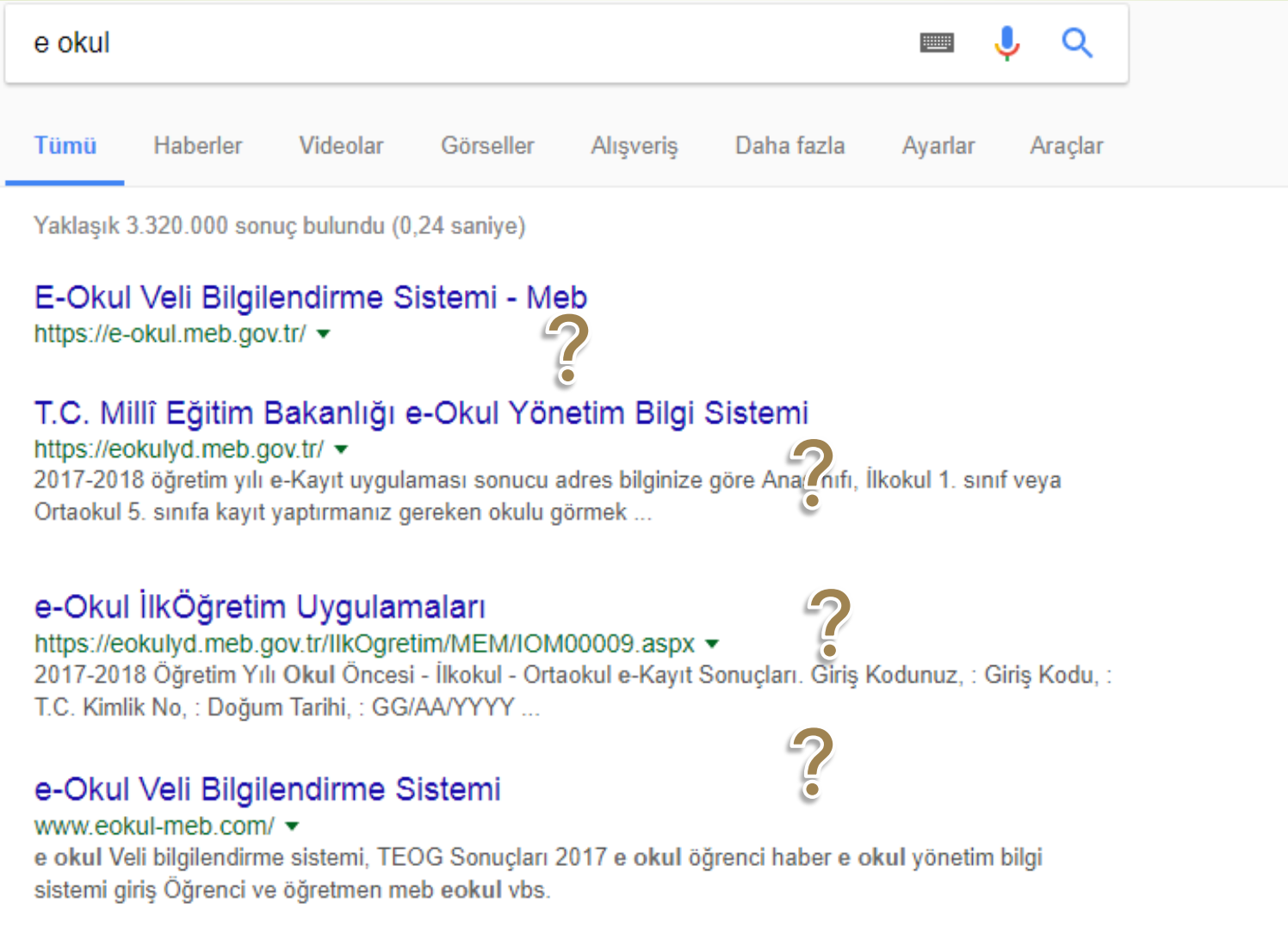
.org: Ticari amacı olmayan vakıf, dernek ve organizasyonların kullandığı uzantıdır.

.edu: Üniversite ve akademik kuruluşların siteleri için kullanılır.

.k12: Okul öncesi, ilkokul, ortaokul ve lise gibi eğitim kurumlarına ait uzantıdır.

- Bilgi edinilen İnternet siteleri, uzantılarına göre değerlendirilerek kaynak güvenilirliği konusunda bir kanıya varılabilir.
- Türkiye Cumhuriyeti'nin İnternet ülke kodu **.tr**'dir. Bu uzantıya sahip sitelere yönelik ülke içinde ayrı bir kontrol gerçekleştirildiği için bu sitelerin güvenilirliklerinin daha yüksek olduğu söylenebilir. Örneğin; Millî Eğitim Bakanlığının İnternet site adresi **meb.gov.tr**, Türkiye Erozyonla Mücadele ve Ağaçlandırma Vakfının adresi de **tema.org.tr**'dir.

Arama Motoru Kullanımı



Adresler incelendiğinde,

Bu adresin Türkiye Cumhuriyeti'ne (.tr) ait bir devlet/hükûmet (.gov) sitesi olduğu görülebilir.

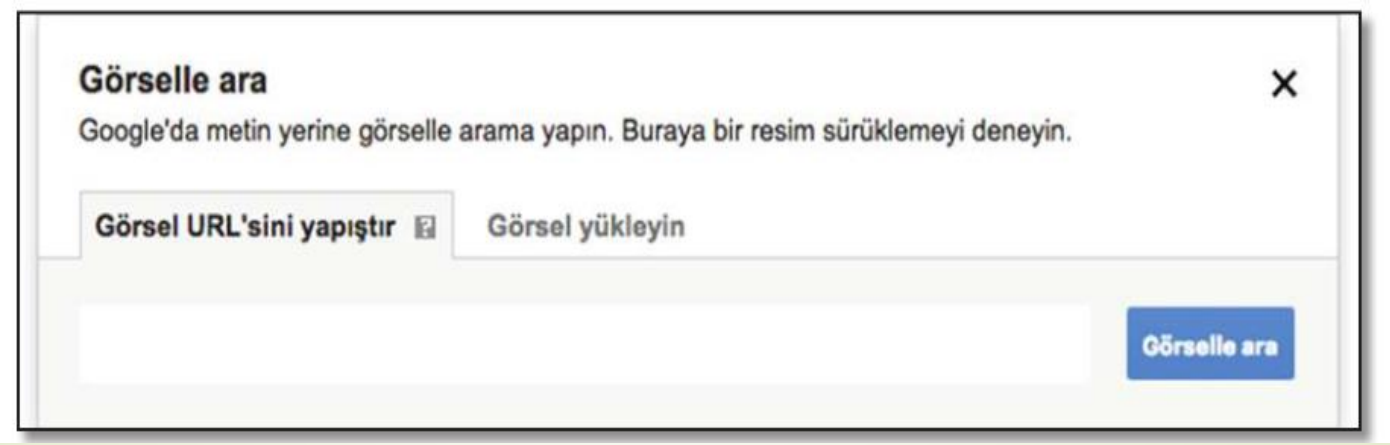
Bu adresin de Türkiye Cumhuriyeti'nde (.tr) faaliyet gösteren bir vakıf ya da derneğe (.org) ait olduğu anlaşılabilir.

Bir arama sitesine "e-okul" ifadesini yazıp listelenen arama sonuçlarını inceleyerek hangisinin e-okul uygulamasının resmî sitesi olduğunu bulunuz.

- Sosyal medyada ya da bazen İnternet sitelerinde çeşitli görseller manipüle edilerek ya da olduğundan çok farklıymış gibi anlatılarak yanlış bilgilendirme, hatta kışkırtma yapılabilmektedir. Böyle durumlarda da görsele dayalı doğrulama yapmak mümkündür.

Bir paylaşım, insanları kışkırtıp şiddet olayları çıkarmak için yapılmış olabilir. Bu tip paylaşımları doğru kabul etmeden önce kontrol edilmek, istenmeyen olayların önüne geçecektir. Bunu anlamak için haberde kullanılan görselin üzerine sağ tıklayıp fotoğrafı bilgisayarınıza indirebilir ya da yine sağ tıklama seçeneklerindeki "bağlantı adresini kopyala" komutunu kullanabilirsiniz.

- Bir arama sitesinin görsel arama sayfasını açıp işaretli yere tıkladığınızda sizden görsel yüklemenizi isteyecektir. Burada, bilgisayarınızda kayıtlı bir görseli yükleyebileceğiniz gibi görselin adresini ilgili alana girebilirsiniz.



Her haber doğru mudur?

Burası Japonya Olsa beğenirdiniz. Ama Burası Bayburt - Of - Çaykara yol ayrımı 😂😂 Beğenmeyecek misiniz 😂😂

See Translation

275 4 Comments 32 Shares


FAKE

“The Castle Island” başlığı altında gördüğünüz mükemmel mimari fotoğraf sonrası Dublin’e gitmek için sabırsızlanıyorsunuz. Ne yazık ki, sahte olan bu fotoğrafı gören milyonlarca insanın inanıp gitmesine neden olmuştur.

Uzun zaman önce, mükemmel viral tanıtımla, mavi karpuz yayınlanmıştı. Mavi ay, Çin, Japon olarak anılan mavi karpuz, insanların oldukça ilgisini çekmişti. Ancak sona kalan, sahte meşrutiyetiydi.

Gebeliğin son zamanlarında; bebeğin tekmelemeleri, karın darbeleri hissedilebilinir. Ancak, fotoğraftaki gibi net bir şekilde bebeğin ayağını görmemiz imkansızdır. Ayrıca fotoğrafa net baktığınızda, doğmamış bir bebek için çok büyük ayağa sahip olduğunu görüyoruz.


FAKE


Sırf bir resim ve yanında bir alıntı var diye
internette okuduğunuz herşeye inanmayın
ABRAHAM LINCOLN

teyit.org

İnternet Etiği

- İnternet kullanımı ile ilgili olarak dikkat edilmesi gereken etik ilkeler; kişilik hakları, özel yaşamın gizliliği ve veri güvenliği gibi başlıklar altında incelenebilir. İnternet ortamında uyulması gereken etik kurallar şunlardır:

- Bize yapılmasından hoşlanmadığımız davranışları başkalarına yapmaktan kaçınmalıyız.

- Bir durum karşısında İnternet'te nasıl davranmamız gerektiği konusunda kararsız kaldığımız zaman gerçek hayatta böyle bir durum karşısında nasıl davranıyorsak öyle davranmalıyız.

- İnternet'te karşılaştığımız ancak yüzünü görmediğimiz, sesini duymadığımız kişilere saygı kuralları çerçevesinde davranmalıyız.

- İnternet sadece belirli bir ırkın, topluluğun ya da ülkenin tekelinde değildir. Tüm dünyadan pek çok farklı kültür ve inanca sahip insan İnternet ortamında varlık göstermektedir. İnternet'i kullanırken her kültüre ve inanca saygılı olmak, yanlış anlaşılabilecek davranışlardan kaçınmak gerektiği unutulmamalıdır.

- İnternet'i yeni kullanmaya başlayan kişilerin yapacağı yanlış davranışlara karşı onlara anlayış gösterip yardımcı olmaya çalışmak ve yol göstermek gerektiği de unutulmamalıdır.

- Özellikle sosyal medya, sohbet ve forum alanlarındaki kişiler ile ağız dalaşı yapmaktan kaçınmalı, başka insanları rahatsız etmeden yazışmaya özen göstermeliyiz. Ayrıca, sürekli olarak büyük harfler ile yazışmanın İnternet ortamında bağırmak anlamına geldiği unutulmamalıdır.
  • İnsanların özel hayatına karşı saygı göstererek kişilerin sırlarının İnternet ortamında paylaşılmamasına dikkat edilmesi gerektiği unutulmamalıdır.
  • İnternet'te kaba ve küfürlü bir dil kullanımından kaçınarak gerçek hayatta karşımızdaki insanlara söyleyemeyeceğimiz ya da yazamayacağımız bir dil kullanmamalıyız.
  • İnternet'i başkalarına zarar vermek ya da yasa dışı amaçlar için kullanmamalı ve başkalarının da bu amaçla kullanmasına izin vermemeliyiz.
  • İnternet ortamında insanların kişilik haklarına özen göstererek onların paylaştığı bilginin izinsiz kullanımından kaçınmamız gerektiği de unutulmamalıdır.

İnternet etiğine uymayan bu davranışlara **siber (dijital) zorbalık** denir. Siber zorbalığa maruz kalmanız durumunda yapmanız gerekenleri şöyle sıralayabiliriz:

- Zorbalık yapan hesaplara cevap vermeyiniz, onlarla tartışmaya girmeyiniz. İlk yapmanız gereken, zorbalık yapan hesabı engellemektir.

- Bu hesapları, bulunduğunuz sosyal medya platformundaki "Bildir/Şikâyet Et" bağlantısını kullanarak şikâyet ediniz. Böylece bu kişilerin size yaptığı etik dışı davranışları başkalarına da yapmasını engellemiş olursunuz.

- Size yönelik etik dışı davranışlar artarak ve ağırlaşarak devam ederse bunların ekran görüntülerini ve mesajları kaydediniz. Bu kanıtlarla birlikte ailenizin ya da rehber öğretmeninizin gözetiminde hukuki yollara başvurunuz.

- Siber zorbalığa maruz kalan başka kişiler de olabilir. Böyle durumlarda bu kişilere ne yapmaları gerektiği konusunda yardımcı olabilir, kötü kullanım bildirimini siz de yapabilirsiniz. Zorba bir hesap için kötü kullanım bildirimi sayısı fazla olursa o hesabın site yönetimi tarafından incelenmesi ve kapatılması daha çabuk olacaktır.

Bilgi Güvenliği

- Kişisel ya da kurumsal düzeyde bizim için büyük 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.

- Bilgi güvenliği, "gizlilik", "bütünlük" ve "erişilebilirlik" olarak isimlendirilen üç temel ögeden meydana gelmektedir. Bu üç temel güvenlik unsurundan birinin zarar görmesi durumunda güvenlik zafiyeti oluşabilir.

- Bilgi güvenliğini oluşturan unsurlardan **gizlilik**, bilginin yetkisiz kişilerin eline geçmemesi için korunmasıdır. Başka bir deyişle gizlilik, bilginin yetkisiz kişilerce görülmesinin engellenmesidir. e-posta hesap bilgisinin bir saldırgan tarafından ele geçirilmesi buna örnek verilebilir.

- **Bütünlük**, bilginin yetkisiz kişiler tarafından değiştirilmesi ya da silinmesi gibi tehditlere karşı korunması ya da bozulmamasıdır. Bir web sayfasında yer alan bilgilerin saldırgan tarafından değiştirilmesi, bütünlük ilkesinin bozulmasına örnek verilebilir.

- **Erişilebilirlik** ise bilginin yetkili kişilerce ihtiyaç duyulduğunda ulaşılabilir ve kullanıma hazır durumda olmasıdır. Bir web sitesine erişimin saldırı sonucunda engellenmesi erişilebilirlik ilkesinin ihlal edilmesine örnek olarak verilebilir.

Bilgi Güvenliğine Yönelik Tehditler

- Bir bilişim teknolojisi sistemine sızmak, sistemi zaafiyete uğratmak, sistemlerin işleyişini bozmak ve durdurmak gibi kötü niyetli davranışlar; **siber saldırı** veya **atak** olarak adlandırılmaktadır.
- Günümüzde siber dendiğinde ilk akla gelen "Sanal Dünya (Internet)" olsa da bir cihazın siber kavramı içinde yer alması için İnternet bağlantısına sahip olması gerekmez.
- **Siber** ya da **siber uzay**; temeli bilişim teknolojilerine dayanan, tüm cihaz ve sistemleri kapsayan yapıya verilen genel addır.

Siber ortamda yaşanabilecek kötü niyetli hareketler:

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 veya iletişim altyapılarına yapılan planlı ve koordineli saldırılardır.

Siber Terörizm: Bilişim teknolojilerinin belirli bir politik ve sosyal amaca ulaşabilmek için hükûmetleri, toplumu, bireyleri, kurum ve kuruluşları yıldırma, baskı altında tutma ya da zarar verme amacıyla kullanılmasıdır.

Siber Zorbalık: Bilgi ve iletişim teknolojilerini kullanarak bir birey ya da gruba, özel ya da tüzel bir kişiliğe karşı yapılan teknik ya da ilişkisel tarzda zarar verme davranışlarının tümüdür.

- **Türkiye'de devlet kurumlarına tahsis edilen 'gov' uzantılı internet siteleri ve e-mail hesaplarına, 12 farklı ülkeden saldırı başladı.**
- Devlet kurumlarının kullandığı ve yalnızca kamu hizmetine tabi olan kuruluşlara tahsis edilen '.gov' uzantılı internet siteleri ve e-postalara karşı, 12 ülkeden eş zamanlı olarak siber saldırı başlatıldı.

  3 gündür süren saldırıların ardından durma noktasına gelen sistemler nedeniyle, birçok e-posta spam olarak algılanmaya başladı.

  GÜVENLİK TEDBİRLERİ ARTIRILDI

  Türkiye'ye gerçekleştirilen siber saldırıların tamamının Güney Kore üzerinden gerçekleştiği iddia edildi ancak uzmanlar bunun sadece IP adresinin kamufle edilmesi nedeniyle böyle göründüğünü vurguladı.

  Avrupa ve Asya kıtalarında bulunan 12 farklı ülkeden geldiği anlaşılan siber saldırılar nedeniyle güvenlik tedbirleri artırıldı.
  http://www.sabah.com.tr/teknoloji/2015/05/14/12-ulkeden-turkiyeye-siber-saldiri

Dünyayı sarsan ağır siber saldırı! Amerika ile Avrupa hedefte...

- **Rus petrol devi Rosneft ve Ukrayna'da hükümete ait bilgisayar ağı dahil olmak üzere birçok sunucu siber saldırıya maruz kaldı. Saldırıların çok ciddi sonuçlara neden olabileceği vurgulandı.**
- Rusya'nın en büyük petrol şirketi Rosneft'in, Ukrayna hükümetinin, ülkedeki bazı bankaların ve başkent Kiev'deki Borispol Uluslararası Havalimanı'nın siber saldırılara maruz kaldığı bildirildi.
- http://www.milliyet.com.tr/rus-petrol-devi-ve-ukrayna-ya-dunya-2475350/

Sayısal Dünyada Kimlik ve Parola Yönetimi

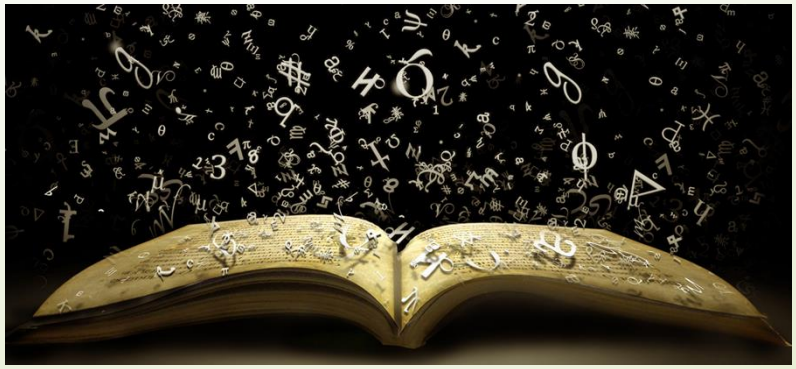
- Her gün sıkça kullandığımız şifre ve parola kavramlarını inceleyecek olursak "**parola**" bir hizmete erişebilmek için gerekli olan, kullanıcıya özel karakter dizisidir. "**Şifre**" ise sanal ortamdaki verilerin gizliliğini sağlamak için veriyi belirli bir algoritma kullanarak dönüştüren yapıdır.
- Sadece rakamlardan oluşan 6 haneli bir parolanın özel programlar yardımı ile dakikalar içinde kırılması mümkündür.
- Saldırganlar, sosyal medya ortamlarını kendi çıkarları için kullanarak sosyal mühendislik adı verilen ikna ve kandırma teknikleri ile bu bilgileri elde edebilirler.

Güçlü bir parolanın belirlenmesi için aşağıdaki kurallar uygulanmalıdır.

- Parola, büyük/küçük harfler ile noktalama işaretleri ve özel karakterler içermelidir.
  • Parola, -aksi belirtilmedikçe- en az sekiz karakter uzunluğunda olmalıdır.
  • Parola, başkaları tarafından tahmin edilebilecek ardışık harfler ya da sayılar içermemelidir.
  • Her parola için bir kullanım ömrü belirleyerek belirli aralıklar ile yeni parola oluşturulması gerekir.

Parolanın güvenliği açısından, aşağıdaki kurallara dikkat edilmelidir:

- Parolanın başkalarıyla paylaşılmaması son derece önemlidir.
  • 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.



PAROLAYI UNUTMAK

- Böyle bir sorun yaşamamak için kullanıcı kendisine özgü kalıplardan yararlanmalıdırlar.
- Örnek olarak;
  Bir anahtar kelime belirlenerek kelime, parola kriterlerine uygun hâle getirilebilir. "Alsancak" kelimesi, parola oluşturma kriterleri göz önüne alınarak "A1s@nc@k" şeklinde düzenlenebilir (8 karakter, büyük harf, küçük harf, sayı ve özel karakter içeriyor.). Bu anahtar kelimenin başına, ortasına ya da sonuna kullanılan platformun kısa ismi eklenerek o hizmete özgü parola oluşturulmuş olur. Twitter için A1s@nc@kTW, Facebook için A1s@nc@kFB gibi.
- - Bir anahtar cümle belirlenerek bu cümlenin bazı harfleri kullanılabilir. Örneğin "Muhtaç olduğun kudret, damarlarındaki asil kanda mevcuttur." cümlesindeki kelimelerin baş harfleri kullanılarak 7 karakter elde edilir. Bu yedi karakterin yanına, kullanılacak platformun kodu da eklendiğinde 9 karakterli bir parola elde edilebilir.
- e-posta hesabı için: M0kd@kM@il, Instagram için: M0kd@kMig gibi…

Anahtar kelime oluştururken;

- G yerine 6,
  g yerine 9,
  Ş yerine $
  a yerine @
  i, l yerine 1 gibi karakterler kullanılabilir.
- Hayalî bir kişinin üç farklı sosyal medya hesabı için güvenli parolalar oluşturunuz.

Kişisel Bilgisayarlarda ve Ağ Ortamında Bilgi Güvenliği

- Bilişim sistemlerinin çalışmasını bozan veya sistem içinden bilgi çalmayı amaçlayan **Virüs, Solucan, Truva Atı ya da Casus yazılım** gibi kötü niyetlerle hazırlanmış yazılım veya kod parçaları zararlı programlar olarak adlandırılır.

- Bu zararlı programlar,
  - 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.

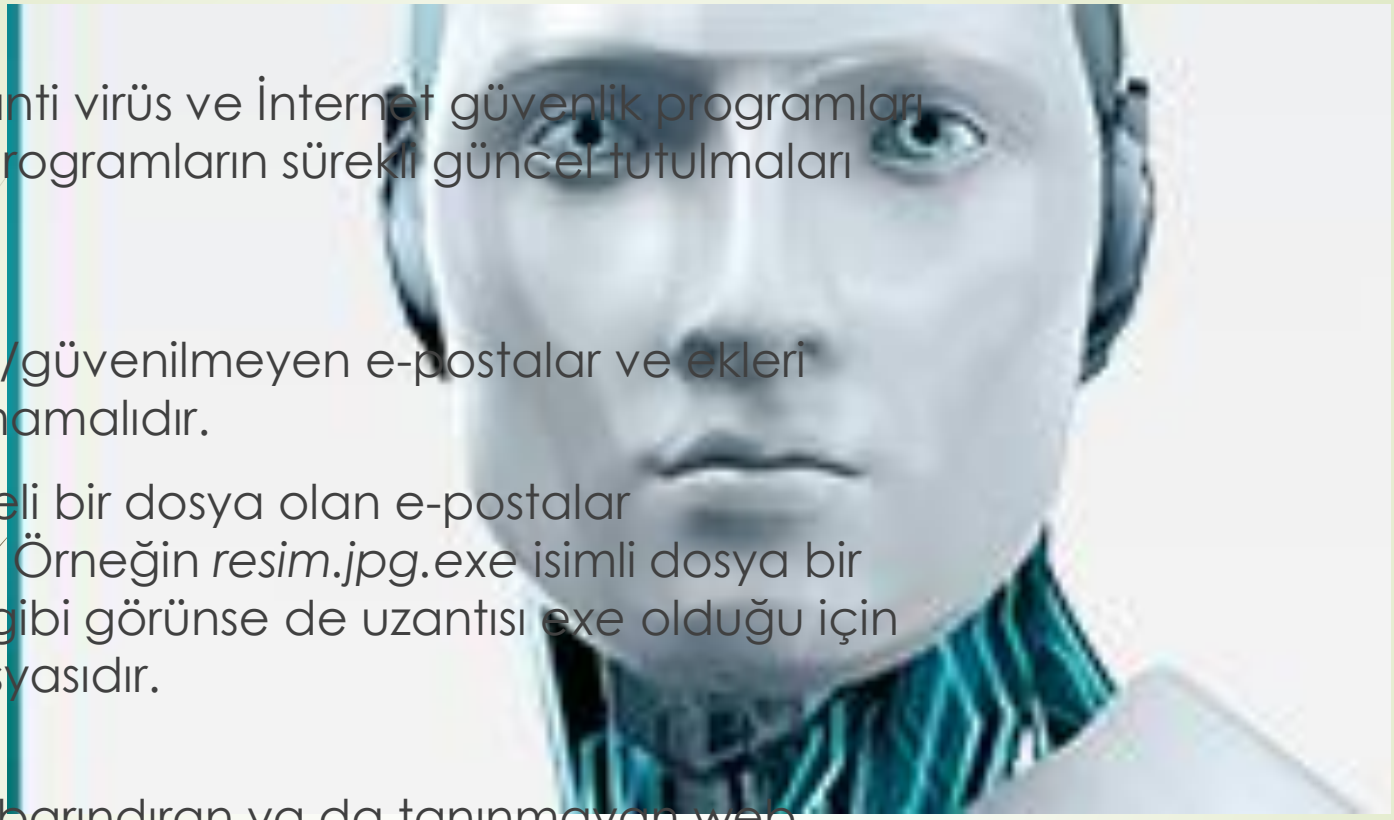
- **Virüsler**, bulaştıkları bilgisayar sisteminde çalışarak sisteme ya da programlara zarar vermek amacıyla oluşturur. Virüsler bilgisayara e-posta, bellekler, İnternet üzerinden bulaşabilir. Bilgisayarın yavaşlaması, programların çalışmaması, dosyaların silinmesi, bozulması ya da yeni dosyaların eklenmesi virüs belirtisi olabilir.

- **Bilgisayar Solucanları**; kendi kendine çoğalan ve çalışabilen, bulaşmak için ağ bağlantılarını kullanan kötü niyetli programlardır. Sistem için gerekli olan dosyaları bozarak bilgisayarı büyük ölçüde yavaşlatabilir ya da programların çökmesine yol açabilir. Ayrıca sistem üzerinde arka kapı olarak adlandırılan ve saldırganların sisteme istedikleri zaman erişmelerini sağlayan güvenlik açıkları oluşturabilir.

- **Truva Atları**, kötü niyetli programların çalışması için kullanıcının izin vermesi ya da kendi isteği ile kurması gerektiği için bunlara Truva Atı denmektedir. Truva Atları saldırganların bilişim sistemi üzerinde tam yetki ile istediklerini yapmalarına izin verir. Sisteme bulaşan bir Truva Atı ilk olarak güvenlik yazılımlarını devre dışı bırakarak saldırganların bilişim sisteminin tüm kaynaklarına, programlarına ve dosyalarına erişmesine olanak sağlar. Güvensiz sitelerden indirilen dosyalar, tanınmayan kişilerden gelen e-postalar ya da taşınabilir bellekler aracılığı ile yayılabilir.

- **Casus Yazılımlar**, İnternet'ten indirilerek bilgisayara bulaşan ve gerçekte başka bir amaç ile kullanılsa bile arka planda kullanıcıya ait bilgileri de elde etmeye çalışan programlardır. Bunlar, sürekli reklam amaçlı pencerelerin açılması ya da İnternet tarayıcıya yeni araçların eklenmesine neden olabilir.

Zararlı Programlara Karşı Alınacak Tedbirler



• Bilgisayara anti virüs ve İnternet güvenlik programları kurularak bu programların sürekli güncel tutulmaları sağlanmalıdır.

• Tanınmayan/güvenilmeyen e-postalar ve ekleri kesinlikle açılmamalıdır.

• Ekinde şüpheli bir dosya olan e-postalar 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.