ETİK, GÜVENLİK VE TOPLUM

Bu sunu bilgisayarbilimleri.com tarafından hazırlanmıştır.

ETİK NEDİR?

- **Etik**; İnsanların yaşadıkları ortamda yaptıkları davranışların doğru ya da yanlış olarak değerlendiren felsefedir.

ETİK ???

- Günlük yaşamda uymamız gereken etik kuralları vardır. Bunlar ile ilgili isterseniz ilk olarak biraz konuşalım ve çeşitli örnekler verelim.

- Bilişim teknolojileri bankacılık, eğitim, sağlık, güvenlik gibi bir çok alanda çok fazla tercih edilmektedir. Hal böyle olunca günlük yaşamımızda nasıl uymamız gereken etik kuralları varsa bilişim teknolojileri alanından da uymamız gereken kurallar vardır.

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.

- Sizce bu etik ilkeler ne olabilir ???

Etik İlkelerin Temel Amaçları

- 1) Bilişim teknolojilerini kullanan insanların yanlış davranış sergilemelerini önlemek
- 2) Bilişim teknolojilerini kullanan insanları güvende tutmak
- 3) Bilişim teknolojilerini kullanan insanların haklarını korumak

ETİK İLKELER

- 1) FİKRİ MÜLKİYET
- 2) ERİŞİM
- 3) GİZLİLİK
- 4) DOĞRULUK

1) FİKRİ MÜLKİYET

- Kişinin kendi zihni tarafından ürettiği her türlü ürün olarak tanımlanmaktadır. Yazılan bir kitap, geliştirilen bir oyun fikri mülkiyet ile ilişkilendirilebilir

Bilişim alanı için geliştirilen yazılımların sahibi kimdir ve kimlerin- kullanımına izin verilmiştir?

Bu sunu bilgisayarbilimleri.com tarafından hazırlanmıştır. Bu sunuyu kullanırken fikri mülkiyet hakkı olarak neler söyleyebiliriz? Şu an bunu sınıfta kullanıyoruz güzel peki izin aldık mı? Telif hakkı sorunu yaşar mıyız?

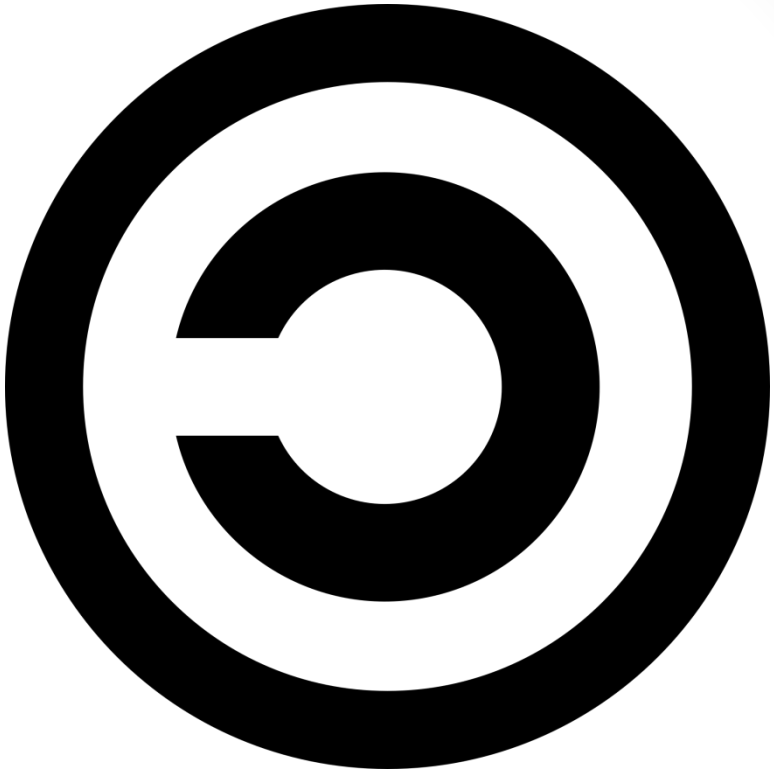
Creative Commons

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

COPY RİGHT

- HER HAKKI SAKLIDIR ☺

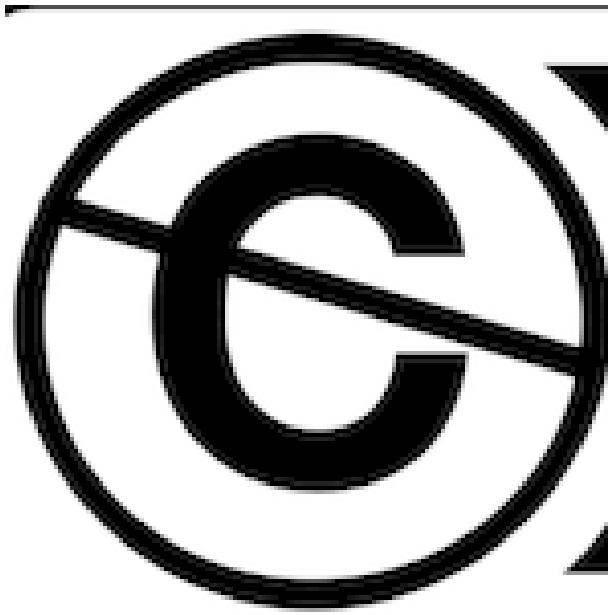
COPY LEFT



Copyright teriminin zıt anlamlısıdır. Eserin telif haklarının belirli bölümlerinden, eser sahibi tarafından belirtilen şartlar altında feragat edilmiş olduğuna işaret eder

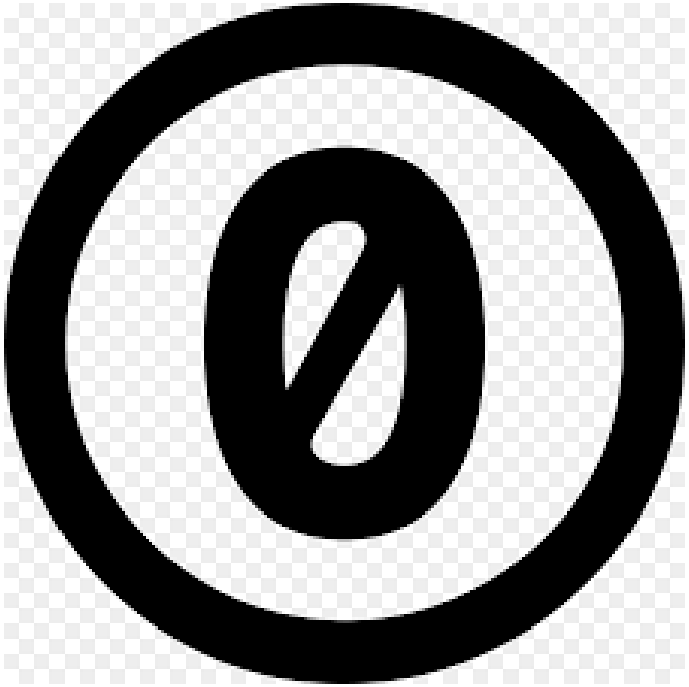
KISACA ☺

KAMU MALIDIR



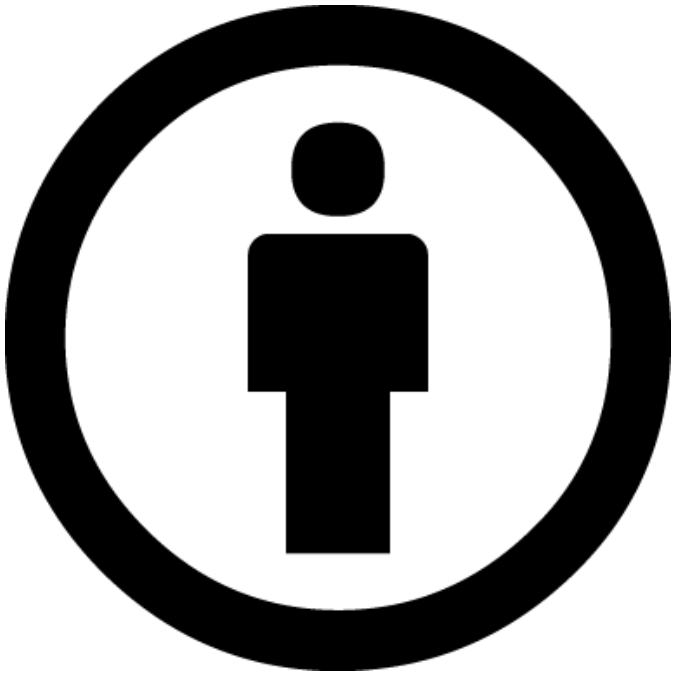
- TELİF SÜRESİ BİTEN ÜRÜNLER KAMU MALIDIR İSTEDİĞİN GİBİ KULLANABİLİRSSİN

Hiçbir Hakkı Saklı Değil



- Hiçbir hakkı saklı değildir istediğin gibi kullanabilirsin

ATIF



- İçeriğini, ürününü aldığın kişiye atıf yapmalısın

- bilgisayarbilimleri.com

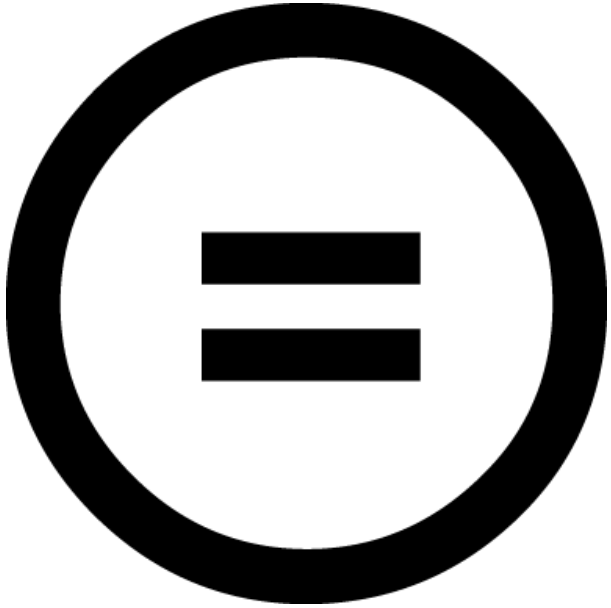
Değiştirip Kopyalayabilirsin

- Aynı lisans türü ile lisanslarsan değiştirip kopyalayıp kullanabilirsin.

Ticari Amaçla Kullanamazsın

- Ürünü ticari amaçla kullanamazsın.

Ürünü türetemezsin



- Yani ürünün üzerinde değişiklik yapamazsın aynı şekilde kullanmak zorundasın

Creative Commons

- 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.

ÖRNEKLER

- Şimdi benim bir ürünüm olduğunu düşünün Bu ürün web sitesi olabilir, herhangi bir oyun olabilir ya da pdf ile hazırlanan bir kitap da olabilir. Şimdi bu ürünlerde yer alan bir den fazla CC lisanslarına bir bakalım

1

2

3

4

5

6

Yukarıda verilen CC lisanlarını doğru bir şekilde eşleştiriniz.

- Atıf yapılmalı, türetilemez, ticari amaçla kullanılamaz.
- Atıf yapılmalı, ticari amaçla kullanılamaz.
- Atıf yapılmalı.
- Atıf yapılmalı, aynı lisans ile paylaşılmalı.
- Atıf yapılmalı, türetilemez.
- Atıf yapılmalı, aynı lisans ile paylaşılmalı, ticari amaçla kullanılamaz.

ONLİNE CEVAPLAYALIM ☺

TIKLA ☺

1

2

3

4

5

6

6 Atıf yapılmalı, türetilemez, ticari amaçla kullanılamaz.

3 Atıf yapılmalı, ticari amaçla kullanılamaz.

1 Atıf yapılmalı.

2 Atıf yapılmalı, aynı lisans ile paylaşılmalı.

4 Atıf yapılmalı, türetilemez.

5 Atıf yapılmalı, aynı lisans ile paylaşılmalı, ticari amaçla kullanılamaz.

LİSANS TÜRLERİ

- **1) ÜCRETSİZ YAZILIMLAR (FREEWARE)**
- **2) LİSANSLI YAZILIMLAR**
- **3) GELİŞTİRME AŞAMASI (BETA)**
- **4) GEÇİCİ KULLANIM (TRİAL)**
- **5)DEMO YAZILIMLAR**


ÜCRETSİZ YAZILIM
(Freeware)
Sizin için güzel bir yazılım yapmaya çalıştım. Ücretsiz istediğiniz gibi kullanın.

LİSANSLI YAZILIM

Önemli olduğunu düşündüğüm yazılımımı belirli bir ücret karşılığında kullanabilirsiniz.


GELİŞTİRME AŞAMASI (BETA)
Bir yazılım geliştiriyorum, yazılımımı deneyip bana fikir vermek ister misiniz?


DEMO YAZILIM
Yazılımım ücretli bir yazılım. Ama bazı özelliklerini kullanabileceğiniz kısıtlı bir sürümünü ücretsiz kullanabilirsiniz.

GEÇİCİ KULLANIM (TRIAL)

Yazılımım ücretli bir yazılım.
İsterseniz 15 gün deneyin,
memnun kalırsanız satın alın.

2) ERİŞİM

- Bilgiye erişim olarak düşünebilirsiniz. İnternet üzerinde yer alan bilgilere erişmeyi ifadeyi etmektedir.

3) GİZLİLİK

- **Özellikle arama motorlarında yaptığımız aramalarda arkamızda eşitli ekmek kırıntıları yani izler bırakırız. Bu izlerde bizlerin gizliliğini tehdit etmektedir.**

ÖRNEK 1

- Örneğin 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. Sadece tarama yaparken değil, birçok kurum ve kuruluşa üye olurken dijital teknolojilerden yararlanıyoruz.

ÖRNEK 2

- Örneğin hastane kayıtları.
- Çoğu hasta hastane kayıtlarının başka kişilerle paylaşılmasını istemez. İşte 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.

duckduckgo.com

DuckDuckGo

duckduckgo.com

- **DuckDuckGo kişisel gizliliğe önem veren bir arama motorudur. Kullanıcıların IP adreslerini kaydetmemektedir. Arama motoru Gabriel Weinberg tarafından ABD'de kurulmuştur. DuckDuckGo Perl dilinde programlanmıştır**

4) DOĞRULUK

- Bilişim teknolojilerini kullanımının doğru bir şekilde olması herkesin sorumluluğu altındadır.
- Uluslararası Bilgisayar Etik Enstitüsüne göre bilişim teknolojilerinin doğru bir şekilde kullanılabilmesi için diğer slaytlarda belirtilen 10 kurala uyulması gerekmektedir.

10 KURAL

- 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.

10 KURAL

- 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.

İNTERNETTE DOĞRULUK

- Günümüzde İnternet kullanıcıları, bilgiye kolay ulaşabilirken amaçları bu olmadığı zamanlarda da sıklıkla bilgi akışına maruz kalmaktadırlar. Bu bilgi akışı her zaman **doğru ve iyi** niyetli olmayabilir. Bu sebeple elde edilen bilgiler kullanılmadan önce bir dizi tedbir almak önemlidir. Bu tedbirler:

- 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.

ALAN ADI UZANTILARI

- .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.

TR

- 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.

ÖZETLE

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.

ETKİNLİK

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

- İnternet sitelerinin adreslerini tanımak, yalnızca doğru bilgiye ulaşmak için gerekli değildir.
- Aynı zamanda karşılaşılabilecek sahtecilik ve bilgi hırsızlığından korunmak için de çok önemlidir.

- Bir önceki etkinlikte e-okul başlığıyla listelenen birbirinden farklı adresler görmüş olmalısınız. e-okul gibi hizmetlere ya da bankaların İnternet sitelerine giriş yaparken bazı özel bilgiler girmeniz gerekir.

- Özel bilgilerinizi girdiğiniz sitenin doğru site olduğundan emin olmalısınız.

- Görselde bir arama sonucunu görmektesiniz. Arama sonuçlarının en üstündeki mavi renkli kısım başlıktır. Arama sonuçlarının başlıkları link/bağlantı niteliğindedir. Yani o kısma tıklandığı zaman ilgili sayfaya gidersiniz.

- Hangi adrese yönlendirildiğinizi arama başlığından değil, başlığın adres bilgisinden anlayabilirsiniz. Görseldeki arama sonucunun başlığına tıklandığında İnternet tarayıcınız www.bilgisayarbilimleri.com sayfasını görüntüleyecektir.

ADRESLER NEDEN ÖNEMLİ

- İnternet ortamında karşılaşılan bilgilerin doğruluğunu teyit etmek ve ayrıca sahteciliğe maruz kalmamak için İnternet sitelerinin adreslerini tanımanın önemini görmüş olduk.

- Özellikle sosyal medya sitelerinde bankaların adına açılan bir çok sahte web sitesini görebilirsiniz. Bu tarz sitelere denk gelince sosyal medya ayarları kısmından ilgili içeriği şikayet ederek kaldırtabilirsiniz. Böylece bilgisiz kişilerin dolandırılmasını da önlemiş olursunuz.

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 ETİĞİ KURALLARI

- 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’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.

- 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.

SİBER ZORBALIK NEDİR

- İnternet etiğine uymayan bu davranışlara denir


SİBER
ZORBA
OLMA!
#FARKINAVAR

- **Siber zorbalık**, çocuklar ya da ergenlerin başka çocuklar ya da ergenler tarafından internet, dijital teknolojiler ya da cep telefonları aracılığıyla eziyet, tehdit, taciz, küçük düşürülme, utandırılma ve benzeri şekillerde hedef alınmasını ifade etmektedir

SİBER ZORBALIK BİR ŞİDDET TÜRÜDÜR.

SANAL ORTAMDA GERÇEKLEŞMİŞ OLMASI, 'GERÇEK' OLMADIĞI ANLAMINA GELMEMEKTEDİR.

Siber Zorbalık Hangi Şekillerde Karşımıza Çıkar?

Mobil cihazlar aracılığıyla başkalarının görüntülerini onların izni olmadan çekip paylaşmak,

Sosyal ağlar ya da sohbet odaları gibi çevrimiçi ortamlarda başkalarına aşağılayıcı, alay edici, öfke dolu, kaba, cinsel taciz veya şiddet içeren mesajlar göndermek,

Bir kişinin kişisel bilgilerini izni ve haberi olmadan internet ortamında paylaşmak,

Siber Zorbalık Hangi Şekillerde Karşımıza Çıkar?

Sosyal ağlarda birisi hakkında dedikodu yaymak ya da özel hayatıyla ilgili konuları herkesle paylaşmak,

Sosyal ağlardaki paylaşımlarına sürekli olumsuz yorumlar yapmak,

Bir kişiye alakalı olarak karalayıcı, aşağılayıcı web sayfaları hazırlamak,

Başkası adına sahte hesap açıp, onun kimliğine bürünmek,

Ortak arkadaşları organize ederek hedef olarak seçilen bireyi, arkadaş listelerinden silmelerini ve engellemelerini, yani sosyal olarak dışlamalarını sağlamak.

Siber Zorbalığı Önlemek İçin Neler Yapabilirim?

- Sosyal ağlardaki hesaplarınıza olan erişimi tanıdığınız ve güvendiğiniz kişilerle sınırlayın,
- Kullandığınız çevrimiçi platformların güvenliğine dikkat edin ve bu ayarları "güvenli" konumda tutun,
- Sosyal ağlarda başkalarının erişimine açık ortamlarda kişisel bilgilerinizi paylaşmayın,
- Hesaplarınıza ait şifrelerinizi arkadaşlarınızla bile paylaşmayın,
- Kaynağına güvenmediğiniz iletileri açmayın, yabancılardan gelen arkadaşlık tekliflerini kabul etmeyin,
- Sinirliyken paylaşım yapmayın,

- Başkasını da ilgilendiren bir içerik paylaşmadan önce onun iznini alın,
- Birini rahatsız edecek türdeki paylaşımların yayılmasına aracılık etmeyin,
- Siber zorbalığa maruz kalırsanız bunu hemen güvendiğiniz bir yetişkinle paylaşın,
- İnternete erişim hakkınızı kullanırken başkalarının haklarını gözetme sorumluluğunuzu unutmayın.
- Dijital dünyada attığınız her adımın gerçek hayatta karşılığı olduğunu unutmayın!

BİLGİ GÜVENLİĞİ

- Günümüzde bilişim teknolojilerinin yaygın kullanımı ile birlikte bilginin üretilmesi ve kullanılması büyük önem kazanmış ve bu teknolojiler aracılığı ile üretilen **veri** miktarında da büyük bir artış olmuştur.

- Bilgisayarlar ve akıllı cihazlar aracılığı ile başta İnternet olmak üzere bilgiye erişimin farklı yollarının ortaya çıkması da bilginin depolanması, iletilmesi ve korunması ile ilgili pek çok problemi de beraberinde getirmiştir.

BİLGİ GÜVENLİĞİ

- **Bilginin ifşa edilmesi, kullanımı, değiştirilmesi, yok edilmesi gibi tehditlere karşı alınan tüm tedbirlere bilgi güvenliği denir.**

BİLGİ GÜVENLİĞİNİ OLUŞTURAN UNSURLAR

- **1) GİZLİLİK**
- **2)BÜTÜNLÜK**
- **3) ERİŞEBİLİRLİK**

GİZLİLİK

- 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.

ERİŞEBİLİRLİK

- 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

- Bilgi ve bilişim teknolojileri güvenliğinde başlıca tehdit, korsan ya da saldırgan olarak adlandırılan kötü niyetli kişiler ve bu kişilerin yaptıkları saldırılardır.

- Bir bilişim teknolojisi sistemine sızmak, sistemi **zaafiyete uğratmak**, sistemlerin işleyişini bozmak ve durdurmak gibi kötü niyetli davranışlar; **siber saldırı** veya atak olarak adlandırılmaktadır.

SİBER NEDİR?

- **Siber** ya da **siber uzay**; temeli bilişim teknolojilerine dayanan, tüm cihaz ve sistemleri kapsayan yapıya verilen genel addır.

- Fiziki sınırları ve kuralları olmayan bu siber dünya içinde yaşanan saldırı, suç, terör, savaş gibi kötü niyetli hareketler daha çok elle tutulur, gözle görülür varlıklarımız için oluşturulmuş kurallar ve yasalar ile engellenemez/korunamaz.

- **Siber ortamda yaşanabilecek kötü niyetli hareketler diğer slaytta tanımlanmıştır:**

- **1) Siber Suç**
- **2)Siber Saldırı**
- **3) Siber Savaş**
- **4) Siber Terörizm**
- **5) Siber Zorbalık**

SİBER SUÇ

- **Bilişim teknolojileri kullanılarak gerçekleştirilen her tür yasa dışı işlemdir.**

SİBER SALDIRI

- **Hedef seçilen şahıs, şirket, kurum, örgüt gibi yapıların bilgi sistemlerine veya iletişim altyapılarına yapılan planlı ve koordineli saldırıdır.**

SİBER SAVAŞ

- **Farklı bir ülkenin bilgi sistemlerine veya iletişim altyapılarına yapılan planlı ve koordineli saldırılardır.**

SİBER TERÖRİZM

- **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.**

SİBER ZORBALIK

- **Bilişim teknolojileri kullanılarak insanların birbirlerine hakaret etmesi, küfür etmesi vb. durumları ifade eder**

Sayısal Dünyada Kimlik ve Parola Yönetimi

- **ŞİFRE NEDİR**
- **PAROLA NEDİR?**

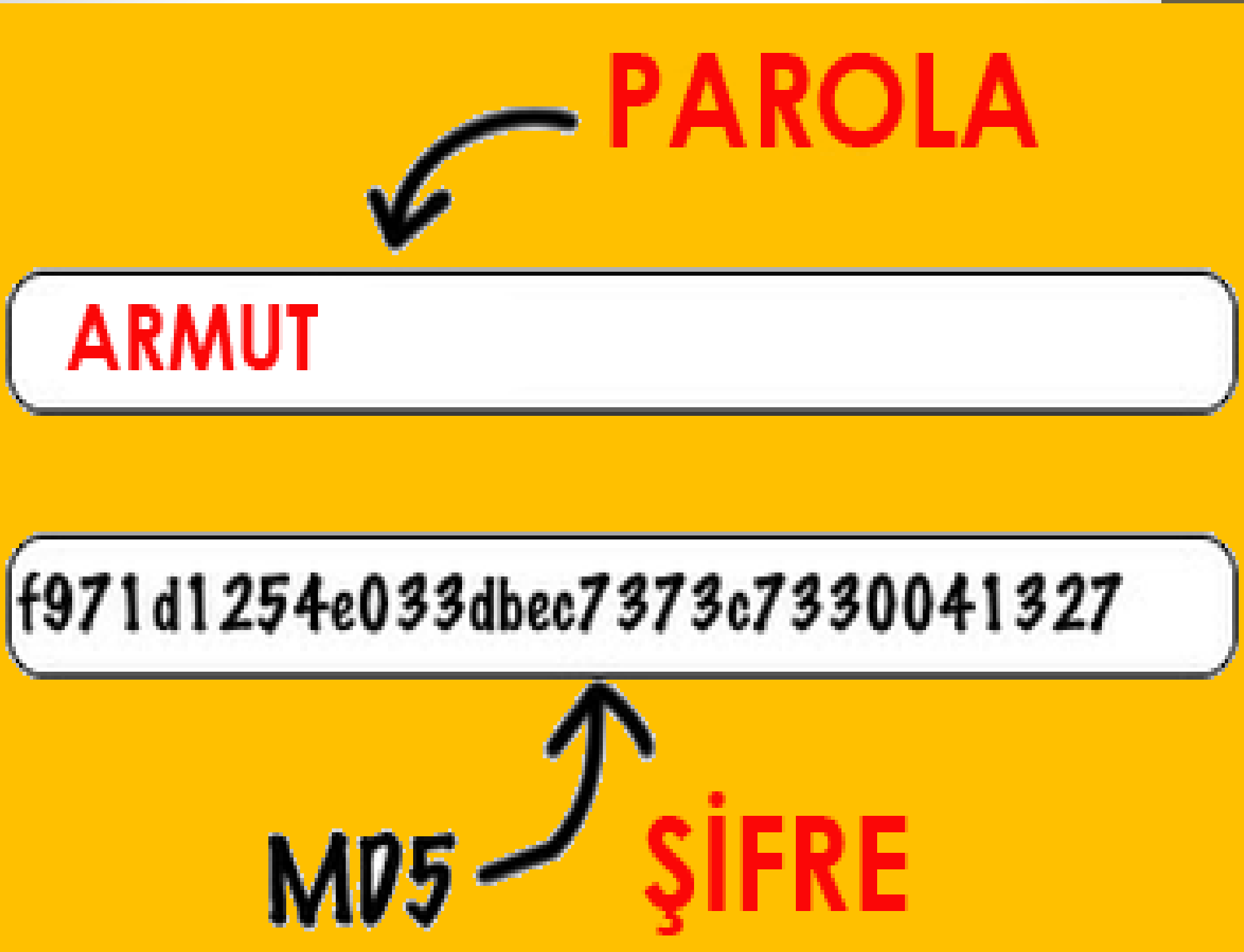

ARZU FİLM

ŞİFRE

- **ŞİFRE :** Normal olarak okunduğunda bir anlam ifade etmeyen, kişiden kişiye farklılık gösteren metinlerin çeşitli algoritmalar ile oluşturulan metinlerdir.

PAROLA

- **PAROLA :** Okunduğunda anlam ifade eden, kişinin kendinin de bildiği, kendinin seçip kullandığı kelimelerdir


PAROLA
ARMUT
f971d1254e033dbec7373c73300413 27
MD5
ŞİFRE

ÖRNEĞİN

- Ortada bir kişi “Face şifreni çok basit yapmışsın, ilk tahmin ettiğim şifre doğru çıktı” gibi konuşmalar yapabilir. Ortamdaki arkadaşlar o duruma belki gülüp geçerler, belki o kişinin adı hacker’a çıkabilir ama şifre ve parolanın farklılığı bilen birisi, “önce sen bir dur. O şifre değil parola” der. ☺

Parola

- Bilgi güvenliğinin en önemli ögesidir. Parolanın da ele geçirilmesi durumunda oluşacak zarar, bir evin anahtarını ele geçiren hırsızın sebep olacağı zarardan çok daha fazla olabilir.

- Parolanın kötü niyetli kişiler tarafından ele geçmesi durumunda,

*Elde edilen bilgiler yetkisiz kişiler ile paylaşılabilir ya da şantaj amacıyla kullanabilir.

*Parolası ele geçirilen sistem başka bir bilişim sistemine saldırı amacıyla kullanılabilir.

*Parola sahibinin saygınlığının zarar görmesine yol açabilecek eylemlerde bulunulabilir.

*Ele geçirilen parola ile ekonomik kayba uğrayabilecek işlemler yapılabilir.

*Parola sahibinin yasal yaptırım ile karşı karşıya kalmasına yol açabilir.

GÜÇLÜ PAROLA İÇİN

- 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.

GÜÇLÜ PAROLA İÇİN

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.

ÖRNEK PAROLA YAPIMI

- “Alsancak” kelimesi, parola oluşturma kriterleri göz önüne alınarak “**A1s@nc@k**” şeklinde düzenlenebilir

- **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.**

123456

123456789

Qwerty

Password

11111

12345678

Abc123

1234567

Password1

1234567890

EN ÇOK KULLANILAN PAROLALAR

ETKİNLİK

- Hayalî bir kişinin üç farklı sosyal medya hesabı için güvenli parolalar oluşturunuz.

Kişisel Bilgisayarlarda ve Ağ Ortamında Bilgi Güvenliği

- Bilişim teknolojilerinin kullanımı her geçen gün artsa da maalesef insanlarımızı bilişim teknolojileri alanlarında yer alan güvenlik ve zararlı yazılımlarla ilgili bilgileri maalesef bilmiyorlar.

- 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.

ZARARLI YAZILIMLAR

- 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.

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.

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.

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 antivirüs 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.

ETKİNLİK

- Zararlı yazılımları ve bu yazılımların ne tür zararlar verebileceğini inceleyiniz.