

Etik Nedir?

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

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

Bilişim teknolojilerinin kullanımında yaşanan etik sorunlar dört temel başlıkta ele alınmıştır.

1-Fikri Mülkiyet: Kişinin kendi zihni tarafından ürettiği her türlü ürün olarak tanımlanmaktadır.

2-Erişim: Sıradan bir vatandaş için herhangi bir bilişim teknolojisi ürününden bilgiye erişebilmesi olarak düşünülebilir.

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

4-Doğruluk : Paylaşılan bilginin doğruluğudur.

 **Creative Commons Nedir?**

Telif hakları konusunda esneklik sağlamak amacıyla, eser sahibinin haklarını koruyarak, eserlerin paylaşımını kolaylaştırıcı modeller sunan, kâr amacı gütmeyen bir organizasyondur.



Ticari Amaçla kullanılamaz



Atıf Yapmak



Aynı Lisanla Paylaş



Türetilemez

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.

ALAN ADI UZANTILARI

.com 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, ilkököl, ortaokul ve lise gibi eğitim kurumlarına ait uzantıdır.

Adresler incelendiğinde,



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



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

Bilgi Güvenliği Nedir?

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.

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

Siber Savunma: Siber ortamda yaşanabilecek suç, saldırı, terörizm, savaş gibi tüm kötü niyetli hareketlere karşı alınacak tedbirler bütünüdür.

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 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.

Parola ve Şifre

"Parola" bir hizmete erişebilmek için gerekli olan, kullanıcıya özel karakter dizisidir.

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.

Zararlı Yazılımlar

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. **Bilgisayar Solucanları**; kendi kendine çoğalan ve çalışabilen, bulaşmak için ağ bağlantılarını kullanan kötü niyetli programlardır.

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 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.

ÖRNEK SORULAR

1-Bilişim teknolojilerinin ve İnternet'in kullanımı sırasında uyulması gereken kuralları tanımlayan ilkelere verilen ad nedir?

-Bilişim Etiği

2-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 tümüne ne ad verilir?

-Siber Zorbalık

3- Temeli bilişim teknolojilerine dayanan, tüm cihaz ve sistemleri kapsayan yapıya verilen genel ada ne denir?

-Siber ya da Siber Uzay

4-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 ne ad verilir?

-Bilgi Güvenliği

5-Bilgiyi doğrulama kurallarını yazınız.

- Kullanıcıya bilgi aktaran kanalın kaynağı belirtmelidir. Kaynağı belirtilmemiş bilgiye şüpheyle yaklaşılmalıdır.
- Elde edilen bilgiler üç farklı kaynaktan teyit edilmelidir.
- Alan adı uzantılarına bakılmalı.



6-Yanda verilen creative commons koşullu lisansının amacı nedir?

-Atıf yapmak

7-Aşağıdakilerden hangisi okul web sitemizin tam adresidir?

-www.pendiktarikbugra.k12.tr

8-IP adreslerini kaydetmeyen ve Gabriel Weinberg tarafından geliştirilen arama motoru sitesi hangisidir?

-Duckduckgo.com

9-Devlete ait resmi kurum sitesine 4 adet örnek veriniz.

www.e-devlet.gov.tr

www.e-okul.gov.tr

www.meb.gov.tr

www.btk.gov.tr

10- Zararlı yazılımlara örnekler veriniz.

Solucan/worm ,Truva , Virüs, Casus yazılım

11- Bulaştıkları bilgisayar sisteminde çalışarak sisteme ya da programlara zarar vermek amacıyla oluşturulan zararlı yazılım hangisidir?

-Virüsler

12-İnternet adresi alan uzantılarından ;

a) Kâr amacı olmayan dernek, vakıf v.b. kuruluş siteleri için kullanılan uzantıyı yazınız. **Cevap: .org**

b) Üniversite siteleri için kullanılan uzantıları yazınız.

Cevap: .edu

c) internet adreslerinde kullanılan ülke kodlarından 3 tanesini yazarak hangi ülkeye ait olduklarını belirtiniz.

Cevap: tr : türkiye , jp : japonya , gr : yunanistan , it : italya, Fr: Fransa , de : Almanya

d) İlk ve orta dereceli okul siteleri için kullanılan uzantıyı yazınız.

Cevap: .k12

e) resmi devlet siteleri için kullanılan uzantıyı yazınız.

Cevap: .gov

13-Zararlı Programlara Karşı Alınacak Tedbirleri yazınız.

- 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.

14-Güçlü bir parolanın belirlenmesi için gereken kurallardan yazınız.

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

15-Güçlü bir parola örneği yazınız.

Örnek 1: @!+Er3N+6547-

Örnek 2: 6oN3n+FE nL153si

Örnek 3: f@cE\$ifrem3324

NOT 1: 11.Soru için verilen örneklerle dikkat ediniz. Sınavda bu örneklerle benzer sizlerde farklı parolalar oluşturunuz.

NOT 2: Bu sorular örnek teşkil etmektedir. Etik, Güvenlik ve Toplum konusundan çıkacak soru tiplerini göstermek için hazırlanmıştır. Soruların birebir aynısı çıkmayabilir. Onun için konuyada çalışmanızı tavsiye ediyorum.