ETİK, GÜVENLİK VE TOPLUM

Etik Değerler

- **Etik**; bireylerin ahlaklı ve ve erdemli bir hayat yaşayabilmesi için hangi davranışlarının doğru, hangilerinin yanlış olduğunu araştıran bir felsefe dalıdır.
- Bir konuya ya da belirli bir meslek dalına özgü etik davranışların tamamı **etik değerler** olarak tanımlanabilir.
- Gelişmekte olan ülkelerde; toplumsal ve bireysel düzeyde artan rekabet ortamı, maddi kazanç sağlama ve bilginin kaynağından çok sonuca odaklanan yaklaşımlar, etiğin geri plana itilmesine yol açmaktadır. 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. 4 ana başlıkta incelenebilir.

  1. Fikrî Mülkiyet: Kişinin kendi zihni tarafından ürettiği her türlü ürün olarak tanımlanmaktadır. Telif hakkı, patent, şifreleme gibi kavramlar da bu başlık altında incelenebilir.

  - "Fikri ve kültürel eserlerden bazıları Creative Commons (CC) organizasyonuna dahildir. CreativeCommons, 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 ön şartıyla belirli kısıtlamalar göz önünde bulundurularak kullanılabilir."

Bilişim Teknolojileri ve İnternet Kullanımında Dikkat Edilmesi Gereken Etik İlkeler

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.

Bilişim Teknolojileri ve İnternet Kullanımında Dikkat Edilmesi Gereken Etik İlkeler

- 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.

Bilişim Teknolojileri ve İnternet Kullanımında Dikkat Edilmesi Gereken Etik İlkeler

Bilişim dünyasında yazılımları lisanslarına göre, özgür yazılımlar ve ticari yazılımlar olmak üzere ikiye ayırabiliriz.

Özgür yazılımlar GPL (General Public Licence - Genel Kamu Lisansı) adı verilen bir lisanlamaya sahiptir. Genellikle ücretsiz olarak (ya da özelleştirilmiş versiyonları düşük ücretlerle) sunulur. En önemli özelliği kaynak kodlarının açık şekilde yayınlanmış olmasıdır. GPL Örneğin; Linux dağıtımları, Libre Office, Google Chrome, GIMP, Notepad++ vb.

Ticari yazılımlar ise çoğunlukla yüksek bedeller (!) karşılığında alınabilmektedir, ticari faaliyet gösteren şirketler tarafından sunulur ve kaynak kodları yayınlanmaz. Örneğin; Microsoft Windows, Microsoft Office, lisanslı oyunlar vb.

Bilişim Teknolojileri ve İnternet Kullanımında Dikkat Edilmesi Gereken Etik İlkeler

Bilişim Etiğinin diğer başlıkları ise şu şekildedir:

2. Erişim: Sıradan bir vatandaş için herhangi bir bilişim teknolojisi ürününden bilgiye erişim olarak düşünülebilir. Bazı durumlarda Fikri Mülkiyet ile çelişebilir.

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. Ancak bilginin aklanması dışında bu bilginin doğru kişilerle doğru zaman diliminde de paylaşılması gizlilik başlığını ilgilendirir. Örneğin hasta, bilgilerini doktoru ile paylaşmak zorundadır.

4. Doğruluk: Bilişim alanında ulaşılan bilgilerin doğru olup olmadığının kontrol edilmesidir.

Bilişim Teknolojileri ve İnternet Kullanımında Dikkat Edilmesi Gereken Etik İlkeler

- 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 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.*

Bilişim Teknolojileri ve İnternet Kullanımında Dikkat Edilmesi Gereken Etik İlkeler

Günümüzde İnternet kullanıcıları, bilgiye kolay ulaşabilirken 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. Örneğin;

.com ya da **.net**: Ticari amaçlı sitelerdir.

.gov: Devlet kurumlarının resmi 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.

Bilişim Teknolojileri ve İnternet Kullanımında Dikkat Edilmesi Gereken Etik İlkeler

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

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.

Bilişim Teknolojileri ve İnternet Kullanımında Dikkat Edilmesi Gereken Etik İlkeler

- Soru : Öğrendiğiniz bilgilere göre **e-okul**'un doğru adresi nedir?

İnternet Etiği

İnternet ortamında uyulması gereken etik kurallar aşağıda verilmiştir:

- Bize yapılmasından hoşlanmadığımız davranışları başkalarına yapmaktan kaçınmalıyız.
- İnternet'te karşılaştığımız ancak yüzünü görmediğimiz, sesini duymadığımız kişilere saygı kuralları çerçevesinde davranmalıyız.
- İnternet'i kullanırken her kültüre ve inanca saygılı olmalıyız.
- 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 Etiği

Siber ortamda yaşanabilecek kotu niyetli hareketler aşağıda tanımlanmıştır:

- **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.

İnternet Etiği

- İnternet etiğine uymayan 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/Şikayet Et” bağlantısını kullanarak şikayet 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.

Bilgi Güvenliği

- Kişisel ya da kurumsal düzeyde bizim için büyük önem teşkil eden her tur bilgiye izin alınmadan ya da yetki verilmeden erişilmesi, bilginin ifşa edilmesi, kullanımı, değiştirilmesi, yok edilmesi gibi tehditlere karşı alınan tüm tedbirlere **bilgi güvenliği** denir.

Sayısal Dünyada Kimlik ve Parola Yönetimi

- 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 hicbir yerde saklanmamalıdır.
- Başta e-posta adresinin parolası olmak üzere farklı bilişim sistemleri ve hizmetler için aynı parolanın kullanılmaması gerekir.

Sayısal Dünyada Kimlik ve Parola Yönetimi

- Güçlü parola oluşturmak için örnek;

Bir anahtar kelime belirlenerek kelime, parola kriterlerine uygun hale 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.

Kişisel Bilgisayarlarda ve Ağ Ortamında Bilgi Güvenliği

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 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.

TEŞEKKÜRLER

Şenol Namaldı