



ÖĞRENME BİRİMİ 1

BİLİŞİM ETİĞİ



Anahtar Kavramlar

Etki, bilişim etiği, kod yazma etiği, sosyal medya etiği, internet etiği, bilgi güvenliği, gizlilik, bütünlük, erişilebilirlik, fiziksel güvenlik, yazılımsal güvenlik, parola güvenliği, <https://>, spam, virüs, dosya, klasör, malware, patent, faydalı model, endüstriyel tasarım, marka, telif hakları, ticari sır

Öğrenme Birimi Konuları

- 1.1. Etik ve Bilişim Etiği Kavramları
- 1.2. Bilgi ve Bilgi Güvenliği
- 1.3. Temel Güvenlik Prensipleri
- 1.4. Fikri ve Sınai Mülkiyet

Bu öğrenme biriminde;

- “Etik” kavramını,
- Bilişim etiğini,
- Bilişimde temel hak ve özgürlükler kavramlarını,
- Kod yazımında dikkat edilmesi gereken etik kavramları,
- Sosyal medya ve internet etiğini,
- Bilgi güvenliği kavramlarını,

- Bilgisayar açılış güvenlik aşamalarını,
- Parola, internet erişimi, e-posta servisleri ve sosyal medya güvenliğini,
- Dosya erişim ve paylaşım güvenliğini,
- Zararlı yazılımlardan korunma prensiplerini,
- Fikrî hakları (telif hakları),
- Sınai mülkiyet haklarını,
- “Ticari sırr” kavramını öğreneceksiniz.

HAZIRLIK ÇALIŞMALARI

1. İnterneti çok kullanıyor musunuz? İnterneti kullanırken etik olmayan bir olayla karşılaşınız mı?
2. Bilgisayarda yaptığınız bir çalışmayı izin almadan inceleyen ve bilgilerinize izinsiz erişen bir yakınınzı olsa nasıl tepki verirsiniz? Böyle bir durumun yaşanmaması için ne yapmalısınız?
3. Bilgisayarınızda kullandığınız işletim sisteme kullanıcı adı ve şifre eklemek güvenliği arttırmır mı? Açıklayınız.
4. Kullandığınız parolaların kolay bulunmaması için ne tür şifreli taktikler kullanıyorsunuz? Açıklayınız
5. Hiç “Akılma gelen bu düşünce bir icat (buluş) olabilir.” dediğiniz oldu mu? Bir şey icat ederseniz hangi yolları izlemeniz gerektiğini biliyor musunuz?

1.1. ETİK VE BİLİŞİM ETİĞİ KAVRAMLARI

1.1.1. Etik ve Bilişim Etiği

Sözlük anlamı olarak etik, ahlak ile ilgili olan kavamları tanımlamaktadır. En çok bilinen altı etik ilke şunlardır: dürüstlük, adalet, ahlak, vicdan, onur ve sorumluluk (Görsel 1.1).

Günümüzde etik, daha çok iş hayatı içinde davranış biçimlerini düzenleyen ve etkileyen bir disiplin olarak yerini almıştır. **Bilişim etiği** ise özellikle bilgisayar kullanımı için ağ ve internet ortamında uyulması gereken kuralları tanımlayan normlar ve kodlar için kullanılmaktadır.

Bilişim etiği, bilişim sektöründe çalışanların dünyanın her yerinde aynı davranış normlarına uymasını sağlayarak hareket etmelerini gerektirir. Bilişim sektörünün gelişmesiyle birlikte ortaya çıkan etik problemlerden bazıları şunlardır:

- Bilgi doğruluğunun sorgulanması
- Özel yaşama ilişkin sorunlar
- Siber suçların ortaya çıkması
- Fikrî mülkiyet hakları
- İşsizlik sorunları
- Sağlık sorunları
- Sosyal ilişkiler ve aile ilişkileri sorunları
- Sanal ortam ve sanal ilişkilerin varlığı
- Yapay zekâ ile ilgili sıkıntıların yaşanması



Görsel 1.1: Sıklıkla kullanılan etik ilkeler

1.1.2. Bilişim Temel Hak ve Özgürlükleri

İnsanlık, bütün önemli tarihî olayların sonucunda daha fazla özgürlük ve temel haklar elde etmek için uğraşmıştır. İnsanca yaşama hakkı, düşünce ve ifade özgürlüğü, özel hayatın gizliliği, haberleşme özgürlüğü ve haber alma hakkı, basın özgürlüğü, bilim ve sanat özgürlüğü gibi temel hak ve özgürlükler ortaya çıkmış; bunlar, devletlerin anayasaları ve uluslararası sözleşmelerinde yer almıştır. Dünyada ve ülkemizde internet teknolojilerine özgü, yeni, birçok suç tipi tanımlanarak kanunlarda yerini almıştır.

Bilişim temel hak ve özgürlüklerinin ihlal edildiği durumlar şunlardır:

- Başkalarının bilgisayarlarına zarar vermek ve bilgisayarlarını bozmak
- Bilgisayarda çalışan insanların çalışmalarına müdahale etmek
- Kişilerin bilgisayar dosyalarını izinsiz almak ve kullanmak
- Bilgisayarda hırsızlık yapmak
- Doğru olmayan bilgileri yaymak için bilgisayar kullanmak
- Korsan yazılım kullanmak
- İzinsiz olarak başkalarının şifrelerini kırmak, kullanmak
- Başkalarının bilgi birimlerini izinsiz olarak kullanmak
- Kötü amaçlı program yazmak

1.1.3. Kod Yazımında Etik İlkeler

Kod yazımında -yazılım geliştirilirken- yazılımcıların uyması gereken etik kuralların kapsamı IEEE [Institute of Electrical and Electronics Engineers (Elektrik ve Elektronik Mühendisleri Enstitüsü)] tarafından belirlenmiştir. Bu etik kurallar aşağıdaki biçimde özetlenebilir:

Yazılımcılar;

- Toplumsal yarar gözetmelidirler.
- İşveren ve müşterinin isteklerini göz önünde bulundurarak projeyi en iyi şekilde yapmalıdır.
- Hem ürün oluşturulurken hem de güncellenirken en son teknolojik standartları kullanmalıdır.
- Ürün oluşturulurken veya gelişimi sırasında hukuki kurallara uymalıdır.

1.1.4. Sosyal Medya Etiği

Günümüzde dünya, küresel bir köye dönüşmüştür. Şüphesiz bunda internet ve cep telefonlarının payı büyüktür. Internetin daha sık kullanılmasıyla sosyal iletişim alanları olarak sosyal medya ağları ortaya çıkmıştır. Sosyal medyanın sık kullanılmasıyla birlikte birtakım kullanıcı odaklı sorunlar artış göstermiştir.

Sosyal medya ağları, her ne kadar siber zorbalık ile ilgili görülen mesajların şikayet edilmesi sistemini geliştirmiş olsa da bu sistemin çok etkili olmadığı gözlenmektedir. Sosyal medyada uyulması gereken etik kurallar şunlardır (Görsel 1.2):

- Taraf tutmamak
- Yalan beyanda bulunmamak
- Toplumun değer yargılarıyla çatışmamak
- Başkaları hakkında asılsız beyanlarda bulunmamak
- Kendini farklı göstermemek
- Açık ve anlaşılır dil kullanmak
- Bağlayıcı açıklamalardan kaçınmak (Kişinin bağlı bulunduğu kurumu, grubu ya da zümreyi dâhil etmemek)



Görsel 1.2: Sosyal medya etiği

- Argo ve küfürden kaçınmak
- Başkalarının özeline saygı duymak

1.1.5. İnternet Etiği

İnternet etiği, gerçek hayatı gösterilen saygının internet ortamında da devam etmesidir. İnternet etiği ile ilgili yazılı olmayan kurallar şunlardır:

- İnternet, kişilerin zararına kullanılmamalıdır.
- Kişilerin yaptığı çalışmalar engellenmemelidir.
- Başkalarının özel dosyalarına izinsiz erişim sağlanmamalıdır.
- Doğruluğu kanıtlanmamış bilgiler desteklenmemelidir.
- Yazılımlar lisanslı olarak kullanılmalıdır.
- Kişilere ait elektronik iletişim kaynakları onların haberi olmadan kullanılmamalıdır.
- İletişim ortamında kullanılacak dilin neden olacağı sorunlar önceden düşünülerek uygun bir dil kullanılmalıdır.



sıra sizde 1.1



Bilişim etiği kavramına uygun olmayan durumlarla ilgili Görsel 1.3'e benzer bir görsel materyal hazırlayınız.

Yandaki GörSEL 1.3 sadece basit bir örnektir. Sizler bilişim etığıne uygun olmayan kod yazımı, sosyal medya etiği ve internet etliğini de kapsayan daha kapsamlı bir görsel materyal hazırlayınız.



ipucu

Web 2.0 araçları ile görsel materyal hazırlayabilirsiniz. Ara- ma motoruna "web 2.0 görsel materyal hazırlama aracı" yaz- diğinizda seçenekler çıkacaktır. Çıkan seçenekleri değerlendi- rebilirsiniz.



GörSEL 1.3: Görsel materyal örneği

1.2. BİLGİ VE BİLGİ GÜVENLİĞİ

Bilgi, insan aklının idrak edebileceği gerçek, olgu ve unsurların hepsine birden verilen addır. Bilişim teknolojilerinde ise bilişim araçları ile işlenmekte olan verilerin tümüne **bilgi** denmektedir.

Bilgi güvenliği; bilgi sahibinin rızası olmadan bilginin yetkisiz olarak elde edilmesini, değiştirilmesini, dışarıya sızdırılmasını, çalınmasını, el değiştirmesini ve bilgiye zarar verilmesini engellemek için alınan önlemler bütünü olarak tanımlanabilir. **Bilgi güvenliği;** gizlilik, bütünlük ve erişilebilirlik olarak

isimlendirilen üç temel ilkeden meydana gelmektedir.

Gizlilik: Erişim izni olmayan kişilerin eline geçmemesi için bilgilerin korunmasıdır. İnternet bankacılığına ait hesap bilgilerinin bir saldırganın (hacker) eline geçmesi, gizlilik ihlaline örnek verilebilir.

Bütünlük: Erişim izni olmayan kişiler tarafından bilgilerin değiştirilmemesidir. Bir web sayfasının içeriğinin değiştirilmesi, bütünlük ilkesinin ihlaline örnek verilebilir.

Erişilebilirlik: İhtiyaç duyulduğunda bilginin erişilebilir ve kullanılabilir durumda olmasıdır. Bir web sayfasına erişimin bir saldırgan (hacker) tarafından engellenmesi, bu ilkenin ihlaline örnek olarak verilebilir.

Bu üç temel güvenlik ögesinden herhangi biri zarar gördüğünde güvenlik zafiyeti oluşmaktadır.



sıra sizde 1.2

“Bilgi güvenliği yönetimi temel kavramları” ile ilgili internette bir araştırma yaparak bilgisayarlarınızda bulunan ya da internetten açacağınız herhangi bir yazım programında, topladığınız bilgileri düzenleyiniz. Araştırmanızı öğretmeninizle paylaşınız.

1.3. TEMEL GÜVENLİK PRENSİPLERİ

1.3.1 Bilgisayar Açılmış Güvenliği

Bilgisayar açılış güvenliği, bilgisayar içinde saklanan verilerin güvenliği anlamına gelmektedir. Bu konuda hem fiziksel güvenlik hem de yazılımsal güvenlik önemlidir (Görsel 1.4). Fiziksel güvenlik, bilgisayarın bulunduğu yerin güvenliğinin sağlanmasıdır. Özellikle taşınabilir bilgisayarlar, kullanılmadığında güvenli bir yerde muhafaza edilmelidir. Dizüstü bilgisayarların çalınması masaüstü bilgisayarlara göre daha kolaydır.



Görsel 1.4: Bilgisayar güvenliği

Bilgisayar açılırken kullanıcı adı ve şifre ayarlanmamışsa fiziksel olarak herkes bilgisayarı rahatlıkla açabilir ve verilere ulaşabilir. İçinde önemli bilgilerin olduğu düşünülen bir bilgisayara mutlaka “kullanıcı adı” ve “parola” atanması gereklidir.

Bilgisayara parola atama işlemi iki şekilde yapılabilir:

- Bilgisayara her açılışta (BIOS) sorması için kullanıcı adı ve şifre ayarlamak
- Bilgisayarda kurulu olan işletim sistemine her açılışında kullanıcı adı ve şifre ayarlamak



sıra sizde 1.3

Aşağıdaki uygulama ve araştırma işlemlerini gerçekleştiriniz.

- a) Şu anda laboratuvarınızda kullanmakta olduğunuz bilgisayara, herkesin kullanıcı adı ve şifresi ortak olmak üzere işletim sistemi üzerinden kullanıcı adı ve şifre veriniz.
- b) BIOS'a kullanıcı adı ve şifrenin nasıl verileceğini internetten araştırınız.

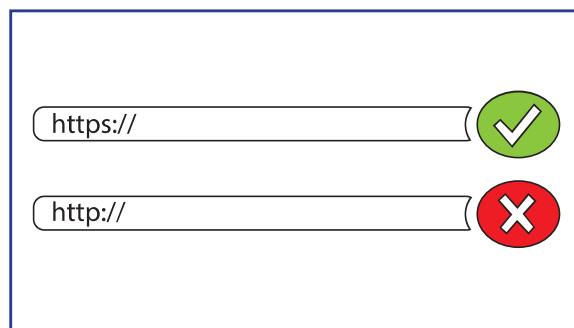
1.3.2 Parola Güvenliği Prensipleri

Basit parolalar verilere izinsiz erişim için açık kapı görevi görmektedir. Kullanılan parolaların tekrar eden ya da sıralı sayılarından oluşması hâlinde tespit edilmesi kolaydır. Günümüzde bankacılık, e-posta, sosyal medya, e-ticaretle ilgili sitelere üye olunurken parolanın sayı, harf ve işaretlerden oluşması istenmektedir. Kavramsal olarak farklı bir parola yapısı oluşturulduğunda bu parolanın çözülmesi daha zordur. **Parola güvenliği için kullanıcılar aşağıdaki hususlara dikkat etmelidir:**

- Tahmin edilmesi zor parolalar kullanılmalıdır (Görsel 1.5).
- Kullanılan parolalar belirli bir metot ile korunmalı ve paylaşılmamalıdır.
- Şifreler belirli aralıklarla değiştirilmelidir. Örnek: Güzel bir "19/Mayıs/95" günü doğum.



Görsel 1.5: Tahmin edilmesi zor bir şifre örneği



Görsel 1.6: https:// ile başlayan sayfalar e-alışveriş için güvenlidir.

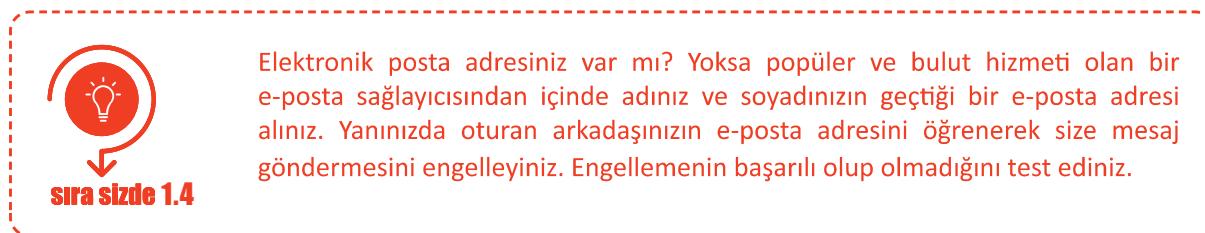
1.3.3. İnternet Erişim Güvenliği

İnternet, insan yaşamını birçok açıdan kolaylaştırmıştır ama dikkatsiz kullanıldığı takdirde önemli sorunlar yaşanabilmektedir. İnternette hangi web sitelerinin güvenli olduğu iyi bilinmelidir (Görsel 1.6). Hassas bilgilerin paylaşımı güvenilir web sayfalarından yapılmalıdır. Tehlikeli olan ve güvenilir olmayan web sitelerine dikkat edilmeli, bilinirliği olmayan web siteleri ziyaret edilmemelidir. **Başında "https://" olmayan siteler e-ticaret için güvenilir değildir.**

1.3.4. E-Posta Güvenliği

E-posta adresi olmayan kişi sayısı günümüzde çok azdır. Bu nedenle e-posta mesajları üzerinden oluşabilecek güvenlik problemleri iyi bilinmelidir. **Spam e-posta mesajları kişilerin izni ve bilgisi dışında iletilen mesajlardır.** Kullanıcılar bu e-postaları ayırt etmekte zorlanmaktadır.

İstenmeyen bu tür e-posta mesajları ile gönderilen bağlantılar ve posta eklerine dikkat edilmelidir. E-posta kutusuna gelen her mesaj açılmamalıdır. Bu tür kullanıcılarından gelen mesajlar, e-postalarda bulunan "engelle" seçeneğiyle engellenmelidir.



1.3.5. Sosyal Medyaya Erişim Güvenliği

Sosyal medya, kişilerin internete bağlanan cihazları kullanarak birbirleriyle sanal bir etkileşim içinde oldukları sosyal ağlara denir. Türkiye'de sık kullanılan sosyal medya platformları; Youtube, Facebook,



Görsel 1.7: Sosyal medya güvenliği

Instagram ve Twitter'dır (Görsel 1.7). Sosyal medya, insanların eğlendiği bir yer olmakla birlikte siber zorbalığın da yaygın olduğu bir alandır. Ayrıca farklı niyetlerle kullanıcıları ağına çekmek isteyen kötü niyetli kişiler de az değildir. **Sosyal medyada her zaman dikkatli bir şekilde iletişim kurup aşağıdaki kurallara uymak gerekmektedir:**

- Resmî olmayan hesapların paylaştığı bilgiler sorgulanmalıdır.
- Kişisel bilgiler, aile hayatı açık bir şekilde gösterilmemelidir.
- Paylaşımının hukuki sorumlulukları bilinmelidir.
- Mesajlaşılan kişilere karşı küfürmeyici, aşağılayıcı, ırkçı veya küfürlü yazılar yazılmamalıdır. Bu yazıların hukuki sorumlulukları unutulmamalıdır.
- Tanınmayan kişiler sosyal ağ hesaplarına eklenmemelidir.
- Fotoğraf ve video paylaşımlarında, içinde yer alan kişilere paylaşım izni alınmalıdır.
- Yer bildiriminde bulunurken arkadaş listesinden emin olunmalıdır.

1.3.6. Dosya Erişim ve Paylaşım Güvenliği

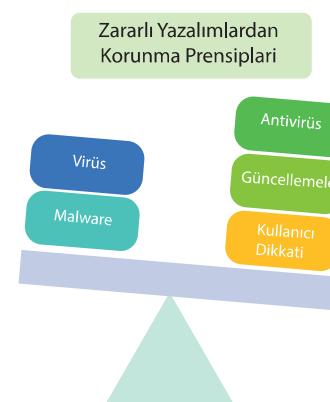
Bilgisayarda yazı, resim ve ses gibi bilgilerin kaydedildiği yapılara **dosya** denir.

Dosyalar Görsel 1.8'deki fiziksel araçlarla paylaşılabilcegi gibi sanal olarak da paylaşılabilir. Dosya sanal ortamdan başkalarıyla paylaşılacaksa bilgisayar için ekstra güvenlik önlemleri alınmalıdır. **Bu güvenlik önlemleri şunlardır:**

- Paylaşılan dosya ve klasörler üzerinde paylaşım sınırlılığı getirilmelidir.
- Önemli olduğuna inanılan dosya ve klasörler şifrelenmelidir.
- Paylaşılan dosyalar için paylaşım görevi bittiğinde paylaşım kaldırılmalıdır. Bunun için bir zaman denetimi yapılabilir.



Görsel 1.8: Dosya erişim ve paylaşım güvenliği



Görsel 1.9: Zararlı yazılımlardan korunma

1.3.7. Zararlı Yazılımlardan Korunma Prensipleri

Tehlikeli ve kötü niyetli yazılımlar İngilizce "malware (malveir)" olarak adlandırılır ve dilimizde de "malware" kelimesi aynı anlamda sık sık kullanılmaktadır. Bu isim, "malicious [malisz (kötü niyetli)]" ve "software [softveir (yazılım)]" sözcüklerinin birleşmesinden oluşmuştur. Zararlı yazılımlar denilince akla sadece virüs gelmemelidir (Görsel 1.9). Virüsler programlara saklanarak ve kendini çoğaltarak dosyaların

bozulmasına veya silinmesine neden olan programcıklardır. Tehlikeli yazılımlar ise bilişim dünyasında var olan tüm risk ve açıklardır.

Tehlikeli yazılımlara karşı önlem almanın temelde 3 yolu vardır:

- 1. Antivirüs:** Bilinen, etkili bir güvenlik uygulaması kullanılmalı ve güncel tutulmalıdır.
- 2. Güncellemeler:** Zararlı yazılımlar, güncellenmemiş ve dolayısıyla açıklar içeren yazılımlarda aktiftir. İşletim sistemi ve programlar güncel tutulmalıdır.
- 3. Kullanıcı:** Güvenliğin sağlanması bilgisayar sahibine önemli sorumluluk düşmektedir. Sorumluluğun yerine getirilmesi için verilen yükümlülüklerin tam zamanında ve doğru bir şekilde yapılması gerekmektedir. Kullanıcının sorumluluklarından biri, şüpheli görünen e-posta eklerini dikkatle incelemesidir. Bir diğer kullanıcı sorumluluğu ise internette alışveriş yaparken hassas bilgilerin güvenilir olan siteler haricinde paylaşılmamasıdır.



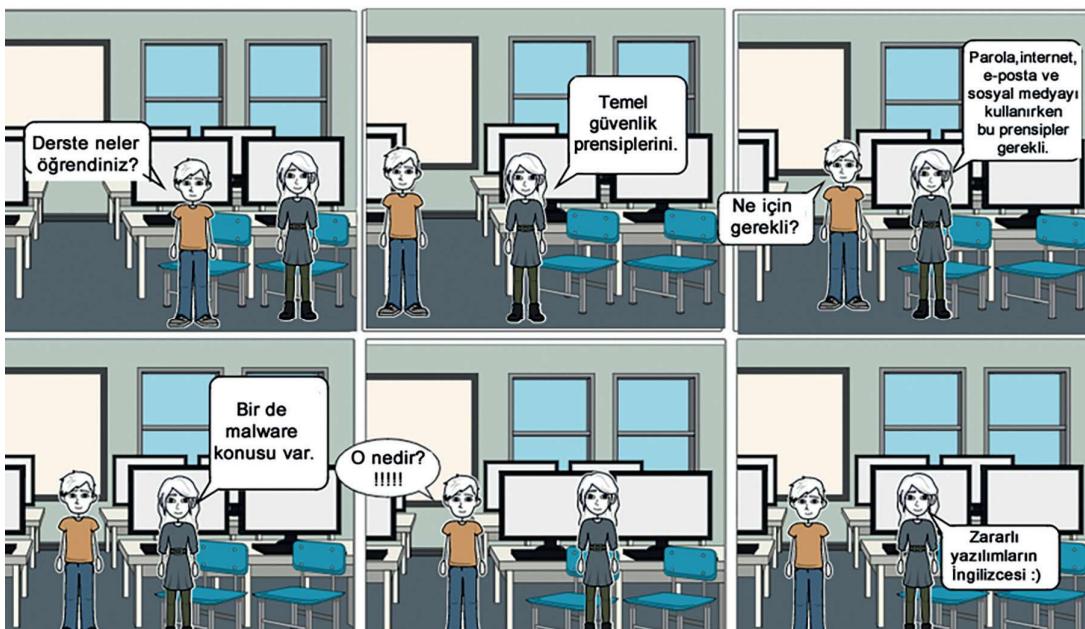
sıra sizde 1.5

Temel güvenlik prensipleri ile ilgili Görsel 1.10'a benzer bir materyal hazırlayınız.



İsterseniz web 2.0 karikatür yapma aracıyla materyal hazırlayabilirsiniz.

Temel güvenlik prensipleri başlığı altında bilgisayar açılış güvenliği, parola güvenliği, internet erişimi, e-posta servisleri, sosyal medyaya erişim güvenliği, dosya erişim güvenliği ve zararlı yazılımlardan korunma prensipleriyle ilgili konuşma yapılan bir ortam hazırlayınız.



Görsel 1.10: Temel güvenlik prensipleri ile ilgili materyal örneği

1.4. FİKRÎ VE SINAİ MÜLKİYET

Fikrî mülkiyet hakları; edebiyat, sanat, müzik, mimari gibi telif hakları olarak isimlendirilen bölümleri; sınai mülkiyet hakları ise sanayi ve teknoloji bölümlerindeki patent, marka ve tasarımları temsil etmektedir (Görsel 1.11). Patent, faydalı model, marka ve tasarım gibi sınai mülkiyet alanındaki hakların Türk Patent Enstitüsü (TPE) tarafından tescil ettirilmesi gerekmektedir.

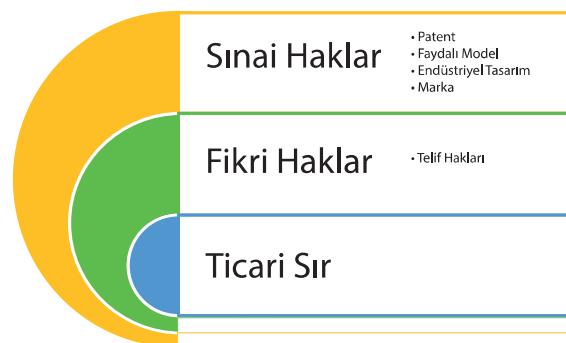
1.4.1. Telif Hakkı

Telif hakkı için eserin, eser sahibinin karakteristik özelliklerini taşıması gerekmektedir. Telif Hakkı Kanunu aynı zamanda bilgisayar yazılımı ve veri tabanları için de koruma sağlar. Telif hakkı pek çok eser türünün korunmasını sağlamaktadır. Bu eserler kişilere aitt;

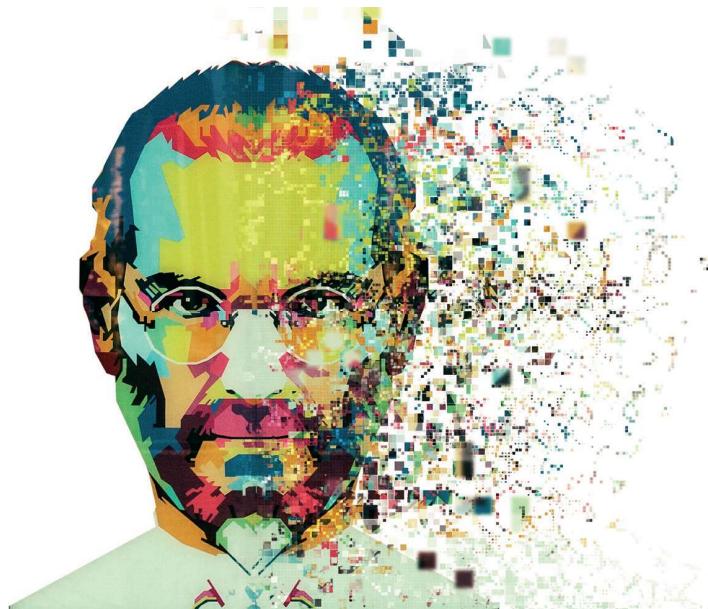
- Televizyon yayınları, filmler ve canlı video yayınları gibi görsel ve işitsel eserler,
- Sesle ilgili kaydedilmiş ürünler,
- Yazılı ürünler (makale türleri, kitaplar, tezler),
- Görsel ürünler (resim, poster),
- Bilgisayar yazılım türlerinin tamamı,
- Tiyatro ürünlerinden meydana gelmektedir.

1.4.2. Marka

Marka, mal veya hizmetleri diğer eş değerlerinden ayırt eden şekillerdir. Kişi adları dâhil sözcükler, şekiller, harfler, sayılar ve malların veya ambalajlarının biçimi gibi her türlü işaret marka olabilir. Günümüzde ses ve koku ile ilgili bazı Türk markaları da koruma altındadır. İlk defa çoklu dokunmatik ekran özelliğini cep telefonlarında kullanarak patentini alan kişi dünyaca ünlü marka sahibi Steve Jobs'tır (Sтив Jobs) (Görsel 1.12).



Görsel 1.11: Fikrî ve sınai mülkiyet hakları



Görsel 1.12: Dünyaca ünlü bir telefon ve bilgisayar markasının sahibi

1.4.3. Patent

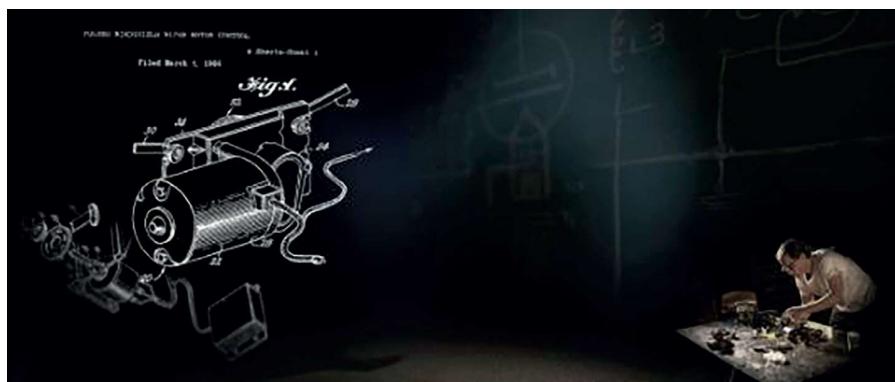
İcat (buluş), önceden kimse tarafından bulunmayan ve olmayan bir şeyin bulunmasıdır. Buluşun özellikleri; yeni bir düşünce, metod ya da araç olması ve yeni bir fikir ile bir soruna çözüm bulması veya önceki fikirlerin geliştirilmiş hâlini sunmasıdır. Patent belgesi; buluş sahibinin, icadının 20 yıl süre ile üretimini yapmasını, kullanmasını ve satışını gerçekleştirmesini sağlamaktadır. Buluş olarak **değerlendirilmeyecek** ürünler de vardır:

- Matematiksel metodlar, bilimsel kuramlar
- Fikrsel olgular, iş çalışmaları
- Bilgisayar yazılımları
- Görsel açıdan albenisi olan ürünler; sanatsal, bilimsel ve edebî ürünler
- Var olan bilginin sunumunun yapılması
- Cerrahi, tedavi ve teşhis prosedürleri
- Konusu toplum düzenine veya genel ahlaki düzene aykırı olan buluşlar
- Bitki ve hayvan yetişiriciliği prosedürleri

Bir Patent Hikâyesi

CAM SILECEKLERİ VE ROBERT KEARNS

1964 yılında Robert Kearns, icat etmiş olduğu “Fasılalı (Zaman Ayarlı) Cam Silecekleri” adlı ürünün patentini aldı. Amerika’da ünlü bir araba markasına ürünü pazarlamak için götürdü ve bu icat, araba markası tarafından çok beğenildi. Araba markası, ürünü almak yerine izinsiz üretmeye başladı ve sonra bir başka araba markası da yine silecekleri izinsiz üreterek satmaya başladı. Robert Kearns bunun üzerine dava açtı ve 1978 yılında her iki şirket 10 milyon dolar tazminat ödemek zorunda kaldı. Önce Amerika’da sonra da tüm dünyada patentin önemi bu olayla daha iyi anlaşıldı ve patent sayıları artmaya başladı. Görsel 1.13’teki bu olayla ilgili 2008 yılında çekilen Flash of Genius adlı filmde bir sahne gösterilmektedir.



Görsel 1.13: Cam sileceklerinin anlatıldığı 2008 çekimi "Flash of Genius" filmi

1.4.4. Faydalı Model

Önceden kamuya sunulmamış, sanayiye uyarlanabilir olan ve uygulamada pratiklik sağlayan modeller **faydalı model** olarak adlandırılır ve ürünü 10 yıl üretme, pazarlama hakkı verilebilmektedir. Faydalı modeller küçük icatlar için daha uygundur. Faydalı modeli kanunlarla koruma sadece ülkemizde var olan bir durumdur. Faydalı modelin korunması ile ilgili haklardan oluşan belgenin verilmesi daha az ücretle ve daha kısa sürede olmaktadır. Görsel 1.14'te faydalı modele verilen bir örnek görülmektedir. Antenli cep telefonları bir icat, daha sonra farklı türlere evrilmesi faydalı modeldir.



Görsel 1.14: İlk cep telefonu buluşu ve sonraki faydalı modeller



sıra sizde 1.6

İlk tıraş bıçağının yapımı buluş, tıraş bıçağına iki kesicili olarak yenilik getirilmesi faydalı modeldir. Sizler de bu şekilde bir buluşa ve faydalı modele örnek veriniz. Verdiğiniz örnekleri materyal şeklinde, "paint" tarzı herhangi bir resim programında Görsel 1.15'teki gibi oluşturunuz.



Tek Kesicili Tıraş Bıçağı bir buluşur.



Görsel 1.15: Buluş ve faydalı model arasındaki fark

1.4.5. Tasarım

Tasarım, bir nesnenin dış görünümü ile ilgili özellikler ve fikirlerdir. Tasarım öncelikle kişilerin görsel algılarını baz alırken diğer algılara yönelik de olabilir. Endüstriyel tasarım tescili ile nesnelerin dekoratif ve estetik özellikleri (çizgisi, şekli, rengi, dokusu, malzemesi, esnekliği) 5 yıla kadar koruma altına alınabilmektedir.



sıra sizde 1.7

Görsel 1.16'da endüstriyel tasarım örnekleri bulunmaktadır. Sizin aklınıza da bir şeyler geldi mi? Nasıl bir tasarım düşünüyorsunuz ve neyin görüntüsünü değiştirmek istiyorsunuz?

- Paint benzeri bir program açınız ve tasarımını yapmak istediğiniz şeyi rastgele çizerek arkadaşlarınıza anlatın.
- Not defteri benzeri bir program açınız ve tasarımını yapmak istediğiniz nesneyi arkadaşlarınıza yazarak anlatın.



Görsel 1.16: Endüstriyel tasarım örnekleri

1.4.6. Ticari Sır

Ticari sırlar, ticari kurumların elde ettikleri başarı ve randımanın oluşturduğu bilgi ve dokümanların üçüncü kişilerin eline geçmemesi ve öğrenilmemesi gerektiği durumlardır. Ticari sırlar gizlilik arz eden bir durumdur.

Çok ünlü bir içecek firmasının içecek formülünün 100 yıldan fazla zamandır korunması bu duruma örnek olarak verilebilir. Ticari sıfır 20 yıl süre ile korunabilmektedir.



sıra sizde 1.8

Öğrendiğiniz tüm Fikrî ve Sînai Mülkiyet Hakkları ile ilgili, görseller ve bir cümlelik notlardan oluşan pano tarzı materyal hazırlayınız.



Arama motoruna "web 2.0 araçları ile görsel materyal hazırlama" yazıldığındá kullanılabilecek birçok program olacaktır. İçlerinden biri seçilerek uygulama gerçekleştirilebilir.

ÖLÇME VE DEĞERLENDİRME

A. Aşağıda verilen cümlelerin başındaki boşluğa cümle doğru ise “D” yanlış ise “Y” yazınız.

1. (....) Dürüstlük, etik ilkeler içerisindeindir.
2. (....) Siber suçların ortaya çıkması, bilişim sektörünün gelişmesiyle ortaya çıkan sıkıntılarından değildir.
3. (....) Lisanslı yazılımlar, istenilen yerden kopyalanıp kurulabilir.
4. (....) Yazılımcılar toplumsal yararı gözetmelidirler.
5. (....) “http” ile başlayan sayfalar internette alışveriş için güvenilirdir.
6. (....) Virüslerin İngilizce adı “malware”dir.
7. (....) Tanınmayan kişiler sosyal ağa eklenmemelidir.
8. (....) Spam e-postalar istenmeyen mesajlardır.
9. (....) Zararlı yazılım, bilgisayar yazılımı ve donanımıyla ilgili her türlü açık ve riskleri ihtiva eder.
10. (....) Antivirüs programı, bilgisayarı risklerden ve tehlikelerden korur.
11. (....) Internetten istenilen programları indirip kurmak riskli değildir.
12. (....) Telif hakları sınai haklar içerisindeindir.
13. (....) Sınai mülkiyet hakları, Türk Patent Enstitüsü (TPE) gibi bir idari kurumda tescil ettirilmelidir.
14. (....) Bir icadın (buluşun) 20 yılına koruma altına alınması işlemeye patent denir.
15. (....) Faydalı model, buluşların şekil değiştirmesidir.

B. Aşağıda verilen soruların doğru cevabını işaretleyiniz.

16. Bilişim temel hak ve özgürlükleri ile ilgili aşağıdakilerden hangisi yanlıştır?

- A) Yazılımlar korsan olarak kullanılmamalıdır.
- B) İzinsiz olarak başkalarının şifrelerine müdahale edilmemelidir.
- C) Başkalarının bilgi birimleri izinsiz olarak kullanılmamalıdır.
- D) Kötü amaçlı program yazmak siber güvenliğe yardımcı olur.
- E) Parolalar kimseye söylememelidir.

17. Aşağıdakilerden hangisi sosyal medya etiği içerisinde yer almaz?

- A) Açık bir dil kullanılmalıdır.
- B) Her arkadaşlık isteği gönderen kabul edilmelidir.
- C) Toplumsal değerlerle çatışılmamalıdır.
- D) Argo sözcükler kullanılmamalıdır.
- E) Çok kişinin yer aldığı fotoğrafların paylaşımı için kişilerden izin alınmalıdır.

18. Aşağıdaki bilgilerden hangisi yanlıştır?

- A) Faydalı model, sadece ülkemizde var olan bir kavramdır.
- B) Fikri haklar içerisine sadece telif hakları girmektedir.
- C) Şirkete ait özel bilginin genelleşmesi ile ticari sırtadan kalkar.
- D) Telif hakkının her sene yenilenmesi gereklidir.
- E) TV şovları, filmler ve çevrimiçi videolar gibi görsel ve işitsel eserler telif hakkına tabidir.

19. Tasarım ile ilgili aşağıda verilen bilgilerden hangisi yanlıştır?

- A) Ürünün görünümü ile ilgili bir özellik ve kavramdır.
- B) Öncelikle insanın görme duyusuna hitap eder.
- C) Endüstriyel tasarım tescili, görünüm özelliklerini koruma altına alır.
- D) Bir nesnenin görsel özellikleri, dekoratif veya estetik bütünü korumaya alınır.
- E) On yıla kadar sahip olma izni alınır.

20. Aşağıdaki parolalardan hangisi parola güvenliği prensiplerine uygun güçlü parola örneğidir?

- A) 246810
- B) Parola
- C) 2020
- D) Qwerty
- E) Z6n7g20!20