F. GÜVENLİK, TELİF HAKLARI VE HUKUK

Konuya Hazırlık

1. Önemli dosyaları yedeklemenin önemini sınıf arkadaşlarınızla tartışınız.
2. Bilgisayar virüsleri hangi yollarla yayılır? Araştırınız.

1. Güvenlik

Bilgisayarda kullanılan mekanik aksam içeren en önemli donanım birimlerinden biri sabit disklerdir. Sabit disklerde büyük miktarda güncel veriler ile programlar bulunur. Bu nedenle sabit disklerin arızalanma riskleri, kullanıcıları, gelişen teknolojiye rağmen hâlen endişelendirmeye devam etmektedir. Çünkü sabit diskin arızalanması sonucu hem veri ve programlar zarar görecek hem de bilgisayar diğer donanım birimleri sağlam olmalarına rağmen çalıştırılamayacaktır. Bilgisayarın bu önemli donanım biriminin içindeki bilgiler bir yandan verimli bir şekilde kullanılmalı diğer yandan da başkalarına karşı korunabilmelidir.

Bir sistemdeki kontrolün yeterli düzeyde olup olmadığını belirlemeye imkân tanıyan başlıca ölçütlerden biri, **verinin (bilgi)** önemidir. Daha önemli bilgileri korumak için, önemsiz olanlara göre, daha fazla para ödenmesi gerekebilir. Her kurum ile her endüstri dalındaki bilgilerin önem ve kritikliği aynı değildir. Korunacak ve kontrol edilecek bilginin değeri, onu korumak ve kontrol etmek için kullanılacak sistemlerin maliyetinden daha yüksek olmalıdır.

a. Dosyaların Taşınabilir Kayıt Ortamlarına Yedeklenmesi

Veri güvenliğinin sağlanabilmesindeki yapılması gereken en önemli faaliyet, yedek alınmasıdır. Bilgisayarda önemli verilerin yedeğinin alınması bir bilgisayar kullanıcısının en önemli görevidir. Yedek alma işlemi dosyaların kopyalarının oluşturulması ile yapılabileceği gibi kullanılan programın otomatik yedek alma menüleri kullanılarak da yapılabilir. Yedek alma işleminde yedeğin kullanılan bilgisayarın dışındaki bir ortama alınması uygun olur. Çünkü herhangi bir problem ile karşılaşıldığında kullanılan bilgisayarda alınan yedek dosyasına da ulaşılamayabilir. Yedek dosyalar taşınabilir bir kayıt ortamına alınmalıdır. Bu kayıt ortamları CD-ROM, DVD-ROM, USB sabit disk, USB flash disk, zip disk vb. olabilir. Yedekleme işlemi, genelde İnternet servis sağlayıcılar tarafından sağlanan ve bulut adı verilen ortak olanlara da yapılabilir.

b. Elektrik Kesintisinde Veri Kaybı

Bilgisayarı oluşturan donanım birimlerinden RAM belleğin sürekli bilgi saklama kabiliyetinin olmadığından daha önceki konularda bahsedilmişti. İşte bu birim elektrik kesintileri karşısında içerisinde bulunan tüm verileri kaybeder. Elektrik kesintilerine karşı alınabilecek bir önlem kesintisiz güç kaynağı (UPS) kullanımıdır. Bu cihaz ile bilgisayarda veri kayıpları önlenebilmektedir. Bankacılık başta olmak üzere birçok alanda bu cihazlar kullanılmaktadır.

Ek Bilgi

Bilgisayar kullanıcısı yaptığı çalışmaları ya sık aralıklar ile kayıt ortamlarına kaydetmelidir.

c. Dosyalara Dışarıdan Erişilmesinin Engellenmesi

Bilgisayarların bir ağ ortamında kullanılması sırasında birbiri arasında dosya alışverişi yapabilmeleri ve birbirinin dosyalarına erişmeleri mümkündür. Dışarıdan bir başka kişinin dosyalara erişiminin önlenmesi için paylaşıma sunulan klasörlerin sınırlandırılması ve bu sınırlandırmanın şifre ile korunması gerekmektedir. Yoksa sabit diskin tümüne verilecek şifresiz bir paylaşımda, başka bir bilgisayar kullanıcısı, ağ ortamını kullanarak bilgisayar içerisinde istediği dosyaya erişip o dosyayı kopyalayıp silebilme imkânı bulacaktır. İnternet ortamında başka bilgisayarlardaki bilgilere izinsiz erişilmesi amacıyla oluşturulan ve bir çeşit virüs olan trojanlar için de gerekli önlemler alınmalıdır.

ç. Gizlilik Hakkı

Hangi nedenle olursa olsun bir başkasının bilgisayarındaki bilgilere izinsiz ulaşılamaz. O kişinin bilgisayarında bir hasara yol açmak ya da dosyalarını ele geçirerek kötüye kullanmak kanunlarımıza göre yasaktır. Bir başkasının bilgisayar sistemine erişim, sabotaj ve engellemeler de suç teşkil etmektedir. Kişisel bilgilerin güvenliğini sağlamak için İnternet ortamından kişisel bilgi alışverişi yapılmaması, banka ve kredi kartı bilgilerinin güvenli olmayan sitelerde kullanılmaması gerekir.

Kişilere karşı işlenen bilgisayar suçları şöyle tanımlanmaktadır:

• Kişilerin rızaları olmaksızın veya kanunların öngördüğü şekil ve usullere uyulmaksızın kişisel verilerin bilgisayar sistemlerine yerleştirilmesine neden olmak,

• Kanuna uygun olarak bilişim sistemlerine yerleştirilmek veya işlenmekle beraber korunmaları için gerekli güvenlik tedbirlerinin alınmaması nedeni ile kişisel verilerin başkasının eline geçmesine veya bozulmasına ya da zarar görmesine neden olmak,

• Kanunun öngördüğü hâller dışında, kişilerin ahlaki nitelikleri, siyasal, felsefi veya dinsel görüşlerini, ırki kökenlerini, sendikal bağlantılarını, cinsel yaşamlarını veya sağlık durumlarını kişisel veri olarak sisteme yerleştirmek,

• Kişisel verileri yetkisiz kişilere vermek, çeşitli özel maksatlarla kullanmak, ele geçirmek.

d. Bilgisayarın Korunması ve Şifrelenmesi

Ek Bilgi

Bilgilerinizin güvenliği için kullandığınız bilgisayarda mutlaka şifre kullanınız.

Bilgisayarları her türlü kötü niyetli kişilerin erişiminden korumak ve gizliliğini sağlamak için şifrelenmesi en uygun çözümdür. Çok değişik şifreleme teknikleri ile kişilerin bilgisayarı açmaları bile engellenebilir. Açılışta çalışan setup programına (BIOS) yerleştirilen şifre ile o bilgisayarı kullanma yetkisi olmayan kişiler bilgisayarı açıp programları kullanamazlar. Bunun dışında dosyalara, klasörlere de değişik tekniklerle şifre verilebilmektedir. Farklı kullanıcaların kullandığı bilgisayarlarda her kullanıcıya basit olmayan farklı şifreler verilmelidir.

2. Bilgisayar Virüsleri

a. Virüslerin Tanıtımı ve Çeşitleri

Çağımızda bilgisayar teknolojisi hızla gelişmektedir. Bilgisayarların bu teknolojik gelişmesinin yanında, bilgisayar programları daha da büyük bir gelişme göstermiştir. Bilgisayarlar önceleri sadece bir hesap makinesi veya bir daktilo makinesi gibi kullanılmıştır. Ancak günümüzde, geliştirilen birçok program sayesinde, her alanda kullanımı kaçınılmaz bir makine hâline gelmiştir.

Bütün bu olumlu gelişmelerin yanında, bilgisayarların kullanımını olumsuz yönde etkileyebilecek bazı programlar da bilgisayar dünyasına girmiştir. Bir bilgisayardan diğerine yayılmak ve bilgisayarın çalışmasına müdahale etmek amacıyla tasarlanmış küçük programlara **virüs** denir. Bir virüs, bilgisayardaki verileri bozabilir veya silebilir, kendisini diğer bilgisayarlara yaymak için kullanıcının e-posta programını kullanabilir, hatta sabit diskteki her şeyi silebilir.

Birçok virüs çeşidi bulunmaktadır. Bunlardan bazıları şöyle sıralanabilir:

1. Dosya virüsleri: Çalıştırılabilir programlara bulaşır ve kendilerini bunlardan diğer dosyalara kopyalar. Dosya virüsleri, virüsten etkilenmiş dosyaların alışverişi sonucu hızla yayılır.

2. BOOT sektör virüsleri: Bu tür virüsler BOOT Record adı verilen küçük yükleyici programa geçer. BOOT Record'a bulaşmış virüs, bilgisayarın işletim komutlarının kontrolünü ile geçirir, her açılışında aktif hâle gelir ve bilgisayara takılan tüm bellek birimlerine kolayca sistemin bulaşır.

3. Trojan: Yerleştiği bilgisayarda yapılan işlemleri izlemek ya da bunlara müdahale etmek için tasarlanmış "exe" uzantılı yazılımlardır.

4. Makro virüsler: Kelime işlemci, veri tabanı, elektronik tablolama programları gibi makro içeren yazılımlarla oluşturulmuş dosyalara bulaşan virüslerdir.

5. Ağ virüsleri: Ağ üzerinde paylaşılan kaynaklar, sürücüler ya da klasörler üzerinden yayılan virüslerdir.

6. Sentineller: Oldukça gelişkin virüs tipi olan bu yazılımlar, bulaştığı bilgisayarın uzaktan kullanma yetkisine sahip olmak amacıyla üretilmiştir.

7. Polimorfik virüsler: Her bulaşmada kendisini değiştiren virüslerdir. Değişiklik rastgele yapıldığından, antivirüs programları tarafından tespit edilmesi de güçtür.

8 Keylogger: Yerleştiği bilgisayardaki klavye kayıtlarını başka bilgisayardan izleyebilmek için tasarlanmış virüslerdir.

b. Bilgisayar Sistemlerine Bulaşması

Bilgisayar virüsleri kişisel bilgisayarlarda daha yaygındır. Bunun nedeni, kişisel bilgisayar kullanıcılarının, birbirlerinden sıkça program alışverişi yapmaları ve güncel anti-virüs programlarını kullanmamalıdır. Bilgisayar virüsleri genellikle USB bellek ve CD-ROM'ların farklı bilgisayarlarda kullanılması sırasında, taşıyıcı programın çalıştırılması yoluyla ya da İnternetten bulaşır. Virüslerin aktif hâle gelebilmesi için çalıştırılabilen (EXE, COM, BAT uzantılı) programlara bulaşması gerekir. Virüs bulaşan bir program çalıştırıldığında, virüs belleğe taşınmış olur. Böylece bilgisayarın belleğine yerleşmiş virüs, çalıştırılan her programa bulaşabilir ve yayılma imkânı bulur.

c. Dosya İndirmedeki Tehlikeler

İnternet'te gezen (sörf yapan) bilgisayar kullanıcısının dikkatli olması gereken en önemli konu bilmediği bir başka bilgisayardan kendi bilgisayarına indireceği dosyalardır. Çünkü bu dosyaların güvenli olup olmadığı bilinmediği veya bir program ile test edilmediği durumlarda bilgisayara virüs ya da trojan bulaşabilir.

İnternet'ten dosya indirirken bilgisayar güvenliği açısından bir sorunla karşılaşmamak için aşağıdaki hususlara dikkat edilmelidir:

1. İnternet'ten mümkün olduğu kadar üreticisi bilinmeyen dosyalar indirilmemelidir. Eğer ilginç yeni bir program kullanılmak istenirse öncelikle başkalarının o program hakkında düşüncelerini öğrenmek için İnternet ve haber grupları araştırılmalıdır.

2. Trojanların, virüsler gibi programlara iliştirilebileceği unutulmamalıdır. Program birinin kişisel sayfasından değil, yapımcının sayfasından indirilmelidir.

3. Virüssüz olduğundan emin olunmayan bir dosya indirilecek olursa her ihtimale karşı ikinci bir koruma önlemi alınması şarttır. Bilgisayara trojanlara karşı koruma sağlayabilen ve sık güncellenen bir antivirüs programı yüklenmelidir.

4. Trojan koruması sağlayan bir anti-virüs programı temin edilemediğinde bilgisayara bir trojan dedektörü yüklenmelidir. Hackerların sisteme ulaşmalarını engelleyen trojan'ların da dışarı veri göndermelerini önleyen programlar kullanılmalıdır.

5. İnternet'te gerekenden fazlası paylaşılmamalıdır. İhtiyaç olmadıkça dosya ve yazıcı paylaşımı (**File and Printer sharing)** programları yüklenmemelidir.

6. Bir network (ağ) üzerinde çalışırken ve dosyalarınızdan bir kısmının paylaşıma açılması gerekiyorsa dosyaların şifre korumalı yapıldığından emin olunmalıdır. "ky8xdj33bgyt67" gibi uzun ve rastgele bir şifre kullanılmalı ve şifre düzenli aralıklarla değiştirilmelidir.

7. Bilgisayar güvenliği alanındaki gelişmeler yakından takip edilmelidir.

ç. Korunma

Bilgisayarı virüsten koruma yolları şunlardır:

1. Bilgisayara, virüs bulaşmadığından emin olunan USB bellek veya CD-ROM takılmalıdır. Bilgisayarlar arasındaki program alışverişini engellemek mümkün değildir. Bu nedenle de herhangi bir USB bellek ya da CD-ROM kullanılacağı zaman öncelikle virüs taraması yapılmalıdır.

2. Virüs temizleme programları kullanılmalıdır.

3. Sabit diske kurulan ve kendini İnternet üzerinden güncelleyen bir anti-virüs programı kullanılmalıdır.

4. Aktif ve güncel bir antivirüs programı olmadan İnternete girilmemelidir.

5. Orijinal paket programların dışında program kullanılmamalıdır.

6. Sabit diske henüz virüs bulaşmamışken programların ve bilgilerin yedeklenmesi yapılmalıdır. Özellikle de **EXE, COM, OVL** uzantılı dosyalar ile önemli verilerin yedekleri kısa aralıklarla alınmalıdır.

7. Bilgisayara takılan USB belleklerin virüslü olup olmadığı kontrol edilmelidir.

8. Virüs kontrolü yapılmamış USB bellekler ile çalışmak zorunda kalındığında disketteki bilgiler, kesinlikle sabit diske kopya edilmemelidir.

3. Telif Hakkı

Bilindiği gibi bir fikir veya sanat eserini üreten kişinin, bu eserden doğan haklarının hepsi, telif hakkı olarak tanımlanmaktadır. Bilgi çağında bilgi toplumu iletişim alanındaki gelişmelerle beraber kendi kurallarını da yazılı hâle getirmeye başlamıştır. Hâlen kontrol edilememe noktasındaki serbestlik ve kişilik hakları, telif hakları gibi önemli konular, ticari uygulamalardaki boşluklar, vergilendirme sistemi gibi birçok geleneksel hukuk konuları, bu yeni toplumsal ortama uygun hâle getirilmeye çalışılmaktadır.

Türkiye'de telif hakkı ile ilgili çok sayıda yasal düzenleme bulunmaktadır. Bunlardan en önemli iki tanesi 1991 yılında Türk Ceza Kanunu'na eklenen "Bilişim Alanında Suçlar" başlıklı 525. madde ve devamında değişiklik yapan kanun ile 5846 sayıl Fikir ve Sanat Eserleri Kanunu'nda değişiklik yapan kanunlardır.

Bilişim suçları, kanunla korunmuş yazılımların izinsiz olarak çoğaltılmasını, yasa dışı yöntemlerle elde edilen bilgisayar yazılımlarının satışını, kopyalanmasını, dağıtımını ve kullanımını ifade eder. Bu suçlar Fikir ve Sanat Eserleri Kanunu'nda eser olarak kabul edilen bilgisayar yazılımlarının, lisans haklarına aykırı olarak kullanılmasını da kapsar.

a. Yazılım Telif Hakkı ve Kopyalama

Herhangi bir yazılımı, hak sahibinin izni olmadan ve telif hakkını ödemeden kopyalamak, lisanssız olarak kullanmak ya da izin verilenden fazla sayıda çoğaltmak gibi eylemler, *yazılım telif hakkı ihlali* olarak adlandırılır. Yazılım korsanlığı (veya yazılım hırsızlığı) olarak adlandırılan bu olay sonucunda üreticiler ve tüm toplum zarara uğramaktadır. Bunun önüne geçmek için kopya yazılım kullanmamak gerekir. Kopya yazılım, kullanan açısından da riskler içermektedir. Bu riskler şöyle sıralanabilir:

- Virüs tehlikesi, bozuk diskler ve hatalı yazılım kullanma,
- Yetersiz dokümantasyon,
- Lisanslı kullanıcılara verilen ürün teknik desteğinden yoksun kalma,
- Lisanslı kullanıcılara sağlanan yeni sürümlere yükseltme imkânına sahip olmama.

Bunlara ek olarak kopya yazılımlar ile yazılım geliştiricinin haklarının dışında, tüm endüstriye zarar verilmiş olunur. Lisansı satın alınan yazılım kullanmanın avantajları şunlardır:

- Virüs tehlikesine karşı korunma,
- Teknik destek güvencesinden yararlanma,

• Doğru ve eksiksiz dokümantasyon rehberliğinde çalışma,

• İhtiyaçlarına özel çözümlere rahatlıkla ulaşabilme,

• Yazılımından daha yüksek verim alma,

• Yazılımını düşük maliyetle güncelleştirme imkânını sağlama,

• Bilgi teknolojilerindeki gelişmeler hakkında sürekli bilgilendirilme.

Yazılım üreticileri, hayatı çok kolaylaştıran bilgisayar programlarını geliştirmek için zaman, para ve çaba harcamaktadırlar. Yatırım ve emeklerinin ürünü olan yazılımların bedellerini onlara değil de kopya yazılım satanlara aktardığımızda ise yeni ürünlerin geliştirilmesi için gereken kaynağı kurutmuş oluruz. Oysa yeni programlar üretmek için yazılım geliştiricilerin bu kaynağa ihtiyaçları vardır. Kopya bir bilgisayar yazılımı alındığında, ödenen para doğrudan yazılım korsanının geliri olur, yazılımın gerçek üreticisi ise hakkını alamaz.

b. Paylaşma ve Ödünç Verme

Lisanslı yazılımlar kullanıcıları tarafından başkaları ile paylaşılması ve ödünç verilmesinde dikkatli davranılması gerekir. Paylaşılan veya ödünç verilen yazılım bu sayede çoğaltılıp kopya sayısı arttırılabilir. Telif haklarına göre suç teşkil eden bu olayın gerçekleşmemesi için lisanslı kullanıcıların özenli davranmaları gerekir. Lisanslı bir kullanıcının sahip olduğu yazılımın kopya sayısının arttırılması lisans sahibini de sorumlu kılacaktır. Lisansların süreleri olduğu da unutulmamalıdır. Lisanslı kullanım süreleri bittiğinde lisans yenilenmelidir. Aksi hâlde yazılım lisanssız kullanılmış olur.

c. Dosyaların Ağ Kanalıyla Transfer Edilmesinin Sonuç ve Yaptırımları

Lisanslı filmlerin, müziklerin, programların ve dosyalarının ağa bağlı bilgisayar kullanılarak başka bir yere transfer edilmesi suç teşkil etmektedir. Telif hakları açısından dosyaların özel programlar kullanılarak transferi bilişim suçları kapsamında değerlendirilmektedir.

Fikir ve Sanat Eserleri Kanunu, bilgisayar suçları ve İnternet aracılığı ile telif haklarına aykırı faaliyetleri de kapsamaktadır. Kanuna göre, eserleri izinsiz olarak kullanan, çoğaltan, işleyen ve bunlara yönelik teknik araçları bulunduran, dağıtan ve bu tip eser ve programları çıkar sağlamak için yayınlayanlar; yayın durdurma, maddi ve manevi tazminatların yanı sıra 71, 72, 73 ve 80. maddelere göre, iki yıldan dört yıla kadar hapis ve on bin TL'den elli bin TL'ye kadar para cezası ile cezalandırılır.

Bu kanunda sorumluluk özel olarak düzenlenmiştir. Buna göre suçun işlenmesine engel olamayan işletme sahibi veya müdürü ve her ne surette olursa olsun işletmeyi fiilen idare eden kimse de cezalandırılır. Bu hukuka aykırı fiillerden dolayı masraf ve para cezasından tüzel kişi de sorumludur.

ç. Paylaşım Yazılımı

Dosya paylaşım yazılımları bir dosyanın farklı kaynaklardan eş zamanlı olarak indirilebilmesini sağlamaktadır. Böyle yazılımlar büyük boyutlu içerik dosyalarını küçük parçacıklara bölerek daha kolay indirilmesini sağlamaktadır. Bu şekilde izinsiz olarak dosya paylaşım yazılımı kullanmak suç olduğundan kitabınızda bu tür programların ismi verilmeyecektir.

Paylaşım yazılımlarından bazılarını kullanarak dosya paylaşan bir İnternet kullanıcısına dünyada ilk kez 2005 yılında Hong Kong'da hapis cezası verilmiştir. Buna rağmen İnternet'in kontrolünün zorluğu nedeni ile dosya paylaşımı programları milyonlarca kişi tarafından kullanılmakta ve her ay yüzlerce yeni müzik albümü ve film bu ağlar üzerinden indirilmektedir. Film ve müzik endüstrisindeki firmalar, bu ağlardan telifli içerikleri ücretsiz olarak sunan ve indirenleri tespit ederek dava açmaya devam etmekte ve çıkacak ağır cezalarla caydırıcı olmaya çalışmaktadır. Ülkeler kendi iç hukukları ve uluslararası hukuk kuralları çerçevesinde konunun çözümü için çalışmaktadır.

d. Kamuya Açık Yazılım

Freeware (ücretsiz) yazılımlar olarak adlandırılan kamuya açık yazılımlar, limitsiz bir şekilde herkes tarafından kullanılabilir. Ancak bu yazılımlar, parayla üçüncü kişilere satılamaz. Böyle bir yazılım kullanan kişilerin yazılım sahibine e-posta ile teşekkür etmesi nezaket icabıdır. Böylece, başka freeware programlar yazma konusunda ve aynı programın yeni sürümlerini hazırlama konusunda programcı teşvik edilmiş olur.

e. Kullanıcı Lisansları

Kullanıcı ile ürün sahibi arasında imzalanan lisans sözleşmesi ile programın kullanımından doğacak hak ve yükümlülükler belirlenmiş olur. Bu belge ile kullanıcı programın kanuni olarak kullanıcısı olur.

Kullanıcı lisans sözleşmelerinde; ürünün kopyalanması, başkalarına verilmesi, ek yazılım hizmetleri, yükseltmeler, firma garantileri gibi konular bulunur. Lisanslı bir program bilgisayara yüklenirken, kullanıcı bir iletişim penceresiyle sözleşme hakkında bilgilendirilir. Yükleme işlemi kullanıcının bu sözleşmeyi okuyarak kabul ettiğini ifade eden düğmeyi tıkladığında devam eder. Bu sayede satın alınmış olan lisanslı yazılım hem firma hem de kullanıcı tarafından onaylanmış olur.

4. Verilerin Kanunla Korunması

Ülkemizde verilerin korunması ile ilgili herhangi bir yasa bulunmamaktadır. Ancak Türkiye'nin, AB sürecinde çıkarmayı taahhüt ettiği Kişisel Verilerin Korunması Hakkında Yasa tasarısı Başbakanlığa sevk edilmiştir.

Kişiye ait her türlü bilgiyi işleyen gerçek ve tüzel kişilerin uyacağı esasları düzenleyen bu tasarının hazırlanılmasında Anayasa'nın özel hayatın gizliliği, konut dokunulmazlığı, haberleşme hürriyeti, Türk Medeni Kanunu'nun kişiliğin korunması, İş Kanunu'nun ve Elektronik İmza Kanunu'nun ilgili maddeleri göz önünde bulundurulmuştur.

DEĞERLENDİRME ÇALIŞMALARI

1. Günlük yaşamımızda en çok kullanılan iletişim teknolojisi ürünleri hakkında bilgi veriniz.
2. Bilgisayar çeşitlerini sıralayarak ağ bilgisayarını açıklayınız.
3. Bilgisayarın hızları hakkında bilgi veriniz.
4. ROM ve RAM bellek kavramlarını açıklayarak bunları karşılaştırınız.
5. Taşınabilir depolama araçları hakkında bilgi veriniz.
6. Bilgisayar kullanılırken gözün ekrandan uzaklığı ne kadar olmalıdır?
7. Bilgisayarın elektrik kablolarının güvenliği hakkında bilgi veriniz.
8. Disket kapasiteleriyle ilgili bilgi veriniz.
9. 512 MB kaç KB eder? Hesaplayınız.
10. Elektronik posta kavramını açıklayınız.
11. Orijinal (lisanslı) olmayan programları kullanmanın ne tür sakıncaları olabilir? Anlatınız.
12. İnternet'ten dosya indirmenin sakıncaları hakkında bilgi veriniz.