Etik, Güvenlik, Toplum

Özet

Bu bölümde;
Bilişim Teknolojilerini kullanırken dikkat edilmesi gereken ilkeleri kavrayacak,
İnternet ortamını etik ilkelere uygun nasıl kullanabileceğinizi anlayacak,
Etik ilkelerin ihlali sonucunda oluşabilecek durumlara örnek verebilecek,
Etik ilkelerin gerekliliğini sorgulayabileceksiniz.

Ali GÖKAŞAR
Bilişim Teknolojileri Öğretmeni

1. Etik, Güvenlik, Toplum

a. Etik Değerler

Etik; bireylerin ahlaklı ve erdemli bir hayat yaşayabilmesi için hangi davranışlarının doğru, hangilerinin yanlış olduğunu araştıran bir felsefe dalıdır. Temelinde barındırdığı güzel ahlaklı, adaletli ve iyi insan olma özellikleri değişmese de zamana, bilimsel gelişmelere ve toplumun gereklerine göre etik kavramına yüklenen anlam değişebilmektedir.

Doğru ile yanlışı, haklı ile haksızı, iyi ile kötüyü, adil ile adil olmayanı ayırt etmek, bunun sonucunda da doğru, haklı, iyi ve adil olduğuna inandığımız şeyleri yapmaktır.

Bir konuya ya da belirli bir meslek dalına özgü etik davranışların tamamı etik değerler olarak tanımlanabilir. Bir alanın evrensel etik değerlerinin belirlenmesi için o alanın toplum tarafından kabul gören ve görmeyen davranışlarının tanımlanması ve bireylerin bunlara uygun davranmalarının sağlanması gerekmektedir. Etik dışı eylemlere ilişkin yaptırımlar, çoğu zaman toplum tarafından belirlenmekte ve bu yaptırımlar gerekirse yasal düzenlemeler için belirleyici olmaktadır.

Günlük hayatımızın vazgeçilmez parçası hâline gelen Bilişim Teknolojileri; **eğitim**, **sağlık**, **medya**, **iletişim**, **ticaret** ve **bankacılık** gibi sektörler başta olmak üzere pek çok alanda yaygın bir şekilde kullanılmaktadır. Bilişim teknolojilerinde yaşanan bu hızlı değişim ve yaygınlaşma, istenen bilgiye her zaman ve her yerde erişebilme imkânı gibi faydalar sunmasının yanı sıra bu teknolojilerin tam olarak anlaşılmadan kullanımına yol açmakta ve bu durum da beraberinde pek çok sorun ortaya çıkarmaktadır.

Bu anlamda yaşanan sorunlardan birisi de zaman ve mekân sınırı olmaksızın erişilen bilginin doğruluğunun ve kaynağının tespitidir. 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. Geleceğin bireylerinin şekillenmesinde bilginin üretilmesi kadar bu bilgilerin etik kurallara göre üretilip paylaşılmasını da sağlamak önem kazanmaktadır. Bu da etiğin ne kadar önemli olduğunu göstermektedir.

Gerçek hayatta insanlara gösterdiğimiz saygı ve nezaketin internet ortamında da gösterilmesi gerekmektedir.

2. 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. Bu ilkelerin temel amacı, Bilişim Teknolojileri ve İnternet'i kullanan bireylerin yanlış bir davranış sergilemesine engel olarak onları güvence altına almaktır. Buna göre **Bilişim Etiği**, Bilişim Teknolojilerinin kullanımı esnasında toplum tarafından kabul gören uyulması gereken kurallar bütünüdür.

Bilişim teknolojilerinin kullanımında yaşanan etik sorunların dört temel başlıkta (fikrî mülkiyet, erişim, gizlilik ve doğruluk) ele alındığı görülmektedir. Aşağıda bu başlıklara kısaca değinilmiştir.

a. Fikri Mülkiyet

Bilgi Kime Aittir?
Bilginin değişimi için gereken ücret nedir?
Bilgi iletişiminin sağlandığı kanallar kime aittir?
Ayrılan bu kaynaklara nasıl erişilebilir?

Bilişim teknolojileri alanında geliştirilen ürünler özellikle yazılım alanında ise arsa, ev, bilgisayar kasası gibi maddi bir varlığın dışında **somut olmayan bir kavramın sahipliği** söz konusu olmaktadır. Bu durumda bu sahipliğin ispatı çeşitli sıkıntılar doğurmaktadır. Aslında günümüzde bu sorunlar müzik, edebiyat alanları için de söz konusudur. Hatta sanat alanındaki bu etik sorun, doğrudan Bilişim Teknolojilerinin gelişmesi ile çığ gibi büyümüştür. Bu tür eserlerin günümüz teknolojisi ile kopyalanıp dağıtılmasının oldukça kolay olması, asıl sahibine dair bilginin korunmasında önemli bir engel olarak

karşımıza çıkmaktadır. "Eserlerin (bilişim alanı için geliştirilen yazılımlar) sahibi kimdir ve kimlerin kullanımına izin verilmiştir?" sorularının cevabı fikrî mülkiyet başlığının altında irdelenmektedir.

Fikrî mülkiyet; kişinin kendi zihni tarafından ürettiği her türlü ürün olarak tanımlanmaktadır. Türk Dil Kurumu ise Bilim ve Sanat Terimleri Sözlüğünde fikrî mülkiyet kavramını "düşünü çalışması sonunda ortaya konulan yazın ve bilim ürünleri üzerindeki iyelik" olarak tanımlamıştır.

Fikrî mülkiyet denince karşımıza hukuki ve etik boyutlar çıkmaktadır. Kimi sorunlar yasal olup etik olmazken kimi de etik olup yasal olmayabilmekte ya da iki boyut birden temelsiz kalabilmektedir. Bu nedenle fikrî mülkiyete ilişkin yasalar, günümüz koşullarına uygun olarak güncellenmeye muhtaç olmaktadır. Telif hakkı, patent, şifreleme gibi kavramlar da bu gereksinim sonucunda ortaya çıkmıştır.

"Fikrî ve kültürel eserlerden bazıları Creative Commons (CC) organizasyonuna dâhildir. Creative Commons, telif hakları konusunda esneklik sağlamayı amaçlayan, eser sahibinin haklarını koruyarak, eserlerin paylaşımını kolaylaştırıcı modeller sunan, kâr amacı gütmeyen bir organizasyondur. Bu organizasyona dâhil olan eserler, kaynağı belirtmek ön şartıyla belirli kısıtlamalar göz önünde bulundurularak kullanılabilir."

Bilişim dünyasında yazılımları lisanslarına göre, özgür yazılımlar ve ticari yazılımlar olmak üzere ikiye ayırabiliriz. Özgür yazılım dünyasına ait GPL'ye (General Public Licence-Genel Kamu Lisansı) sahip yazılımlar ücretsiz olarak (ya da özelleştirilmiş versiyonları düşük ücretlerle) kullanılabilirken, ticari faaliyet gösteren firmaların ürettiği yazılımların lisanslarıysa çoğunlukla yüksek bedeller karşılığında alınabilmektedir. Kişi ya da kuruluşlar yazılım seçimi yaparken ihtiyaçlarını doğru şekilde belirledikten sonra tercih yapmalıdır. Böylece yüksek maliyet ödemekten ve beklentileri karşılamayan program edinmiş olmaktan kaçınmış olurlar.

Lisanssız yazılım kullanmanın etik uygunsuzluk yanında teknik sakıncaları da vardır. Firmalarca sunulan yazılımlar, zaman zaman güvenlik açıklarını kapatmak ya da ek özelliklerle donanmak amacıyla güncelleme alır. Lisanssız kullanılan yazılımlar, bu güncellemeleri alamaz ve bilgi güvenliği açısından bilgisayarları savunmasız kılar.

b. Erişim

Bu başlık bilgiye erişimi anlatmaktadır. Sıradan bir vatandaş için herhangi bir bilişim teknolojisi ürününden bilgiye erişim olarak düşünülebilir. Erişim aynı zamanda şahsi ve gizli verilere yetkisiz erişimi engellemek için geliştirilen önlemleri de içerir.

Hangi bilgi, bir insan veya organizasyon tarafından doğrudan veya ayrıcalıklı olarak, hangi güvenlik ve koşullar altında elde edilir?

Örneğin herhangi bir arama sitesini kullanarak, istediğimiz bilgiye hızlıca erişebiliriz. Ancak bilgi daha özel bir formatta sunulmuş olabilir. Örneğin bir veri tabanında saklanıyor olabilir. Bu durumda karşımıza üç sorun çıkmaktadır:

Bilgiye erişebilecek düzeyde bilişim bilgisi,
Bilginin yararlılığını test edecek düzeyde bilgi okuryazarlığı,
Bilgiye erişmenin varsa maddi karşılığı olan ekonomik güç.

Günümüz insanı birinci sorunu aşmakta oldukça başarılı gibi görünürken, ikinci sorunun aşılmasında hâlâ güçlükler söz konusudur. Çünkü bilgi yığınları artmakta ve bu bilginin doğruluğunu test etmek güçleşmekte ayrıca son kullanıcı dediğimiz vatandaşın bunu test etme bilincinin eğitilmesi gerekmektedir. Üçüncü sorun olan ekonomik boyut için kütüphane veri tabanları bir çözüm olarak karşımıza çıkmaktadır. **Bu durumda bilginin ücretsiz olması "Herkesin eşit derecede bilgiden yararlanmasını sağlar." çözüm önerisi, fikrî mülkiyet ile çelişecektir.**

c. Gizlilik

Bir önceki başlıkta bahsettiğimiz gibi, bir arama sitesi kullanarak bilgiye hızlıca erişim, herhangi bir kişi için sıradan bir davranış hâline gelmiştir. Bugün herkes aklına gelen her şeyi özgürce Google ya da Yandex gibi arama motorlarında aramaktadır. Oysa ki her arattığımız şey ile birlikte hatta bilişim ortamında yaptığımız her eylem ile ardımızda "ekmek kırıntısı" olarak tabir edilen izler bırakıyoruz. Eğer

birilerinin bizim bu bıraktığımız ekmek kırıntılarını takip ettiği hissine kapılırsak ne kadar rahatsız olacağımızı bir düşünün.

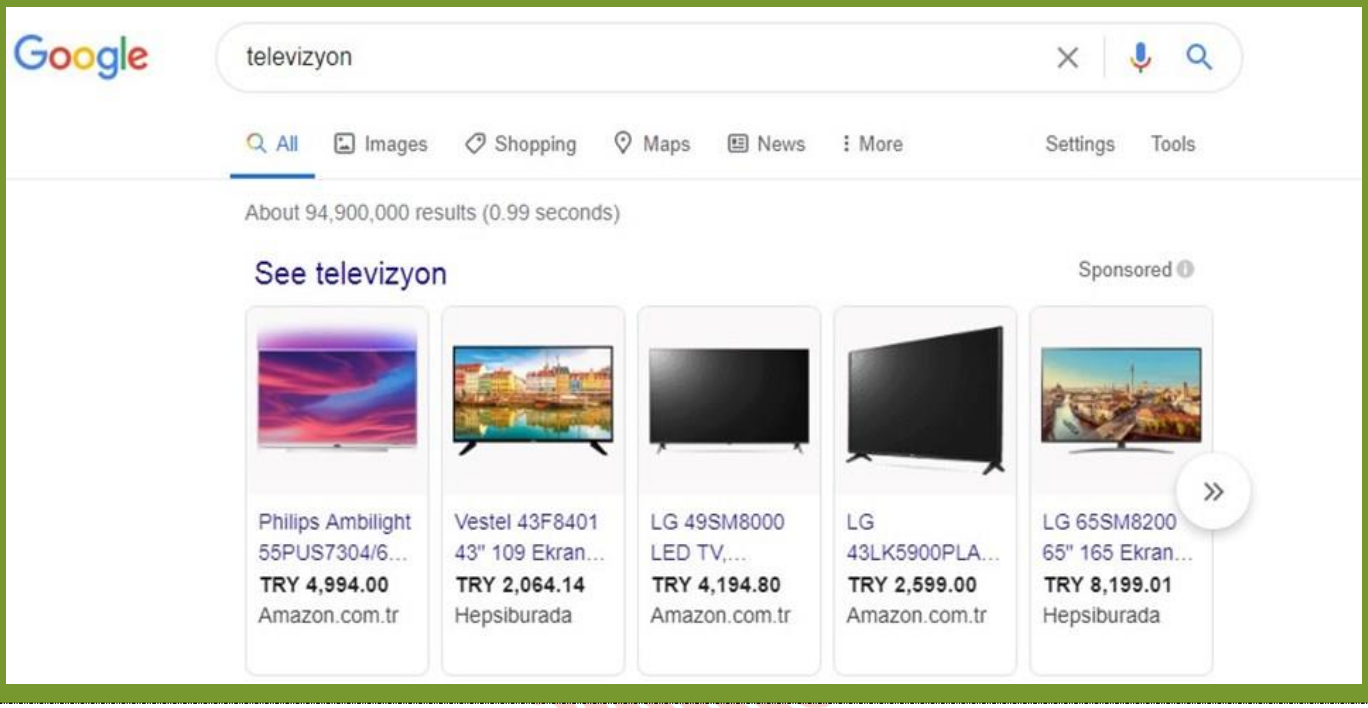
Örneğin Google'da arama yaparken karşınıza çıkan reklamların, sizin daha önce ziyaret ettiğiniz siteler ve bunların içeriklerinden elde edilen verilerle tespit edilen ilgi alanlarınıza yönelik olduğunu görmüşsünüzdür.

Güncel Bilgi

Google, Türkiye'de Alışveriş Reklamlarını Kaldırıyor

Arama motoru Google, Rekabet Kurulu kararı sonrası 10 Ağustos 2020'den itibaren, arama motorlarında çıkan alışveriş reklamlarını kaldırma kararı aldığını duyurdu.

Söz konusu karar kapsamında 10 Ağustos itibari ile Google'a satın almak istediği bir ürünün ismini yazan kullanıcılar, artık arama sayfasının en üst kısmında çıkan slider şeklindeki alışveriş reklamlarını görmeyecek.



Sadece tarama yaparken değil, birçok kurum ve kuruluşa üye olurken dijital teknolojilerden yararlanıyoruz. 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. Ancak bilginin saklanması dışında bu bilginin doğru kişilerle doğru zaman diliminde de paylaşılması gizlilik başlığını ilgilendirir. Örneğin hasta, bilgilerini doktoru ile paylaşmak zorundadır.

İzlenmekten kaçınmak için açık kaynak dünyasından alternatifler kullanılabilir. Örnek olarak https://duckduckgo.com sitesini inceleyiniz

d. Doğruluk

Tahmin edilebileceği gibi bilişim alanında şahsımıza ait bilgiler bizim dışımızdaki kişiler tarafından da kayıt altına alınabilmektedir. Ancak bu bilgilerin doğruluğu kimin sorumluluğundadır? Biz kendimize ait bilgileri kontrol etme hakkına sahip olmalıyız ve kendimize ait bilgileri kendimiz kodlayacaksak bunun sorumluluğunu da üstlenmek zorundayız. Ayrıca anonim bilgilerin doğruluğunun sorumluluğu kimde olmalıdır?

Örneğin, içeriğini kullanıcıların oluşturduğu bilgi paylaşım siteleri (wiki ortamları) açık sistemlerdir. Bu sistemlerdeki verilerin doğruluğunun garantisi kimdedir gibi sorular bu başlık altında ele alınmaktadır.

Uluslararası Bilgisayar Etik Enstitüsüne göre bilişim teknolojilerinin doğru bir şekilde kullanılabilmesi için aşağıda belirtilen 10 kurala uyulması gerekmektedir.

Bilişim teknolojilerini başkalarına zarar vermek için kullanmamalısınız
Başkalarının bilişim teknolojisi aracılığı ile oluşturduğu çalışmaları karıştırmamalısınız
Başkasına ait olan verileri incelememelisiniz
Bilişim teknolojilerini hırsızlık yapmak için kullanmamalısınız
Bilişim teknolojilerini yalancı şahitlik yapmak için kullanmamalısınız.
Lisanssız ya da kırılmış/kopyalanmış yazılımları kullanmamalısınız
Başkalarının bilişim teknolojilerini izinsiz kullanmamalısınız.
Başkalarının bilişim teknolojileri aracılığı ile elde ettiği çalışmalarını kendinize mal etmemelisiniz.
Yazdığınız programların ya da tasarladığınız sistemlerin sonuçlarını göz önünde bulundurmalısınız.
Bilişim teknolojilerini her zaman saygı kuralları çerçevesinde kullanmalı ve diğer insanlara saygı duymalısınız.

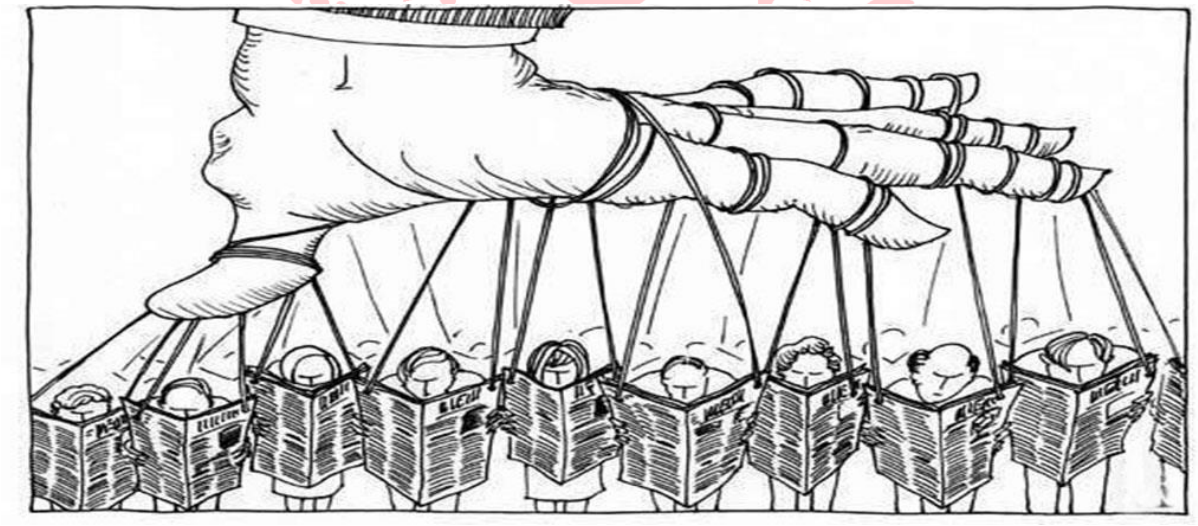
"Eskiden bir bilgiye ihtiyaç duyulduğunda kitaplara, ansiklopedilere başvurulurdu. Şimdi ise, sosyal medya sitelerinden bilgi toplanıyor."

Yeni iletişim teknolojilerinin yoğun bir şekilde hayatımıza girmesiyle birlikte, "bilgiye ulaşmak" hiç olmadığı kadar kolaylaşırken, bu kolaylık, pek çok sorunu da beraberinde getirdi. Bu sorunların başında; yalan haberlere maruz kalma, yanlış veya şüpheli bilgiyi yayma eğilimi, manipülasyon ve bunların sonucunda oluşan "bilgi kirliliği" geliyor.

Yalan haber ve manipülasyon, bugüne özgü, internetin varlığıyla oluşmuş bir tartışma değil ve her zaman vardı fakat günümüzde "yanlış bilginin yaygın bir şekilde paylaşılması, yalan haber ve bilgi kirliliği" dijital medya ortamlarında çok daha yoğun bir şekilde karşımıza çıkıyor.

i. Sosyal Medya-Yalan Haber İlişkisi ve Medya Okur Yazarlığı

Giderek artan sosyal medya kullanımı, toplumdaki her bireye düşüncelerini paylaşabilme olanağı sunuyor. Bunu pozitif ve lehimize bir durum olarak görsek de manipüle edici, provoke edici, yalan ve yanıltıcı bilginin yayılması açısından bakıldığında durum pek de iç açıcı değil!



Sosyal medyada yalan haber ve yanlış bilginin, "eğlence veya siyasi propaganda amacıyla" dolaşıma sokulduğunu düşünenlerin yanı sıra, yaşanan bilgi kirliliğinin "kötü niyetli çevreler tarafından kasıtlı yapıldığını" söyleyenler de var. Dünyada ve ülkemizde sosyal medya aracılığıyla yaşanan toplumsal, siyasi olaylara ve çeşitli terör olaylarına bakıldığında, üretilen bilgi kirliliğinin, propaganda amaçlı olduğu ve bu işin örgütlü bir şekilde, kitleleri harekete geçirmek, kamu düzenini bozmak ve zarar vermek amacıyla oluşturulduğu görülüyor.

Oxford Üniversitesi bünyesindeki Reuters Gazetecilik Çalışma Enstitüsü'nün 2016 Dijital Haberler Raporu'nda Türkiye, 26 ülke arasında "sosyal medyanın bir haber kaynağı olarak görülmesinde" yüzde 73'lük oranla ikinci sırada yer alıyor.

İşte asıl mesele de burada başlıyor. Sosyal medyanın, kişisel hesaplardan anında yapılan paylaşımlar nedeniyle, haberin bireylere ulaşmasında zaman ve hız açısından avantajlı olduğu bilinse de güvenilirlik, doğruluk, manipüle etme (Çıkarlar doğrultusunda yönlendirme) bilgiyi çarpıtma ve çevrimiçi radikalleşme konularında tehlike oluşturduğu su götürmez bir gerçek.

Bilen ile bilmeyen, iyi veya kötü, doğru ile yalan, enformasyon ile dezenformasyon arasındaki farkın belirsizleştiği sosyal medya ortamlarında, popüler kültürün ve trendlerin etkisiyle paylaşım rüzgârına kapılan herkes; **kaynağı bilinmeyen bilgilere, videolara, ses kayıtlarına ve haberlere, muhakeme etmeden inanıyor ve bunları düşünmeden paylaşıyor.** Dolayısıyla da var olan bilgi kirliliğine hizmet etmiş oluyor. Bu sebeple yalan haber, günümüzde mücadele edilmesi gereken ciddi sorunların başında geliyor.

Yalan haberle mücadelenin temel taşı, her ne olursa olsun bilgiye kolayca ulaşmaya çalışmak değil, **"doğru ve güvenilir bilgiye"** ulaşmak için çabalamaktır. Peki, hangi bilgi doğru ve güvenilir, bunu nereden bileceğiz? Bunun için biraz zaman ayırmak ve önemli bazı kullanım alışkanlıkları edinmek gerekiyor.

Öncelikle **"Eleştirel bir bakış açısı edinmek", "doğrulanmamış bilgileri paylaşmamak"**, özellikle sosyal medyada karşılaşılan **"bilgilere sağlıklı bir şüphe ile yaklaşmak"** ve **"bilgiye ulaşılan kaynaklar hakkında fikir sahibi olmak"** yalan haberle mücadele kapsamında yapılması gerekenlerin başında geliyor. Bunlara ilaveten paylaşım yapmadan önce **"genel bir araştırma yapmak ve ulaşılan bilgileri en az 3 farklı güvenilir kaynaktan teyit etmek"** de doğru bilgiye ulaşmanın olmazsa olmazını oluşturuyor.

Bazı web siteleri parodi, reklam veya sahte haber yapma ve yayma amacıyla kuruluyor. Sosyal medyada zaten "troll" olarak adlandırılan, art niyetli kişi ya da grupların bu işe kendilerini adadıkları biliniyor. Yani, sadece yalan haberler ve resimler üretmek ve sosyal paylaşım ağlarında insanları yanıltmak ve yönlendirmek amacıyla çalışan pek çok insan var(!). Tek başına bu bilgiye sahip olmak bile, "**Neden internet ortamında her bilgiye inanmamalıyız**?" sorusunu cevaplamaya yetiyor.

İnternet Okuryazarlığı konusunda gerekli donanıma ve bilince sahip olunmadığı takdirde, İnternetteki yalan ve yanıltıcı haber, resim ve videolara inanma ihtimali çok yüksek.

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.

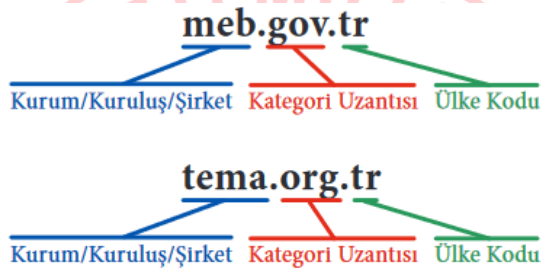
- Bilgiyi aktaran İnternet sitesinin adresi kontrol edilmelidir. Alan adı uzantıları birçok İnternet sitesi için fikir verebilir. Örneğin;

.com ya da .net : 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.

Bilgi edinilen İnternet siteleri, uzantılarına göre değerlendirilerek kaynak güvenilirliği konusunda bir kanıya varılabilir. 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.

Adresler incelendiğinde;



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 tıklandığında bir İnternet adresine yönlendirilirsiniz. Hangi adrese yönlendirildiğinizi arama başlığından değil, başlığın altındaki yeşil renkli adres bilgisinden anlayabilirsiniz. Görseldeki arama sonucunun başlığına tıklandığında İnternet tarayıcınız https://giris.turkiye.gov.tr sayfasını görüntüleyecektir. Arama sonuçlarında görüntülenen diğer kısım olan siyah renkli metindeyse siteye ilişkin tanıtıcı bilgi ve açıklamalar görülebilir.

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

Bundan ayrı olarak özellikle sosyal medyada ya da bazen İnternet sitelerinde çeşitli görseller manipüle edilerek ya da olduğundan çok farklıymış gibi anlatılarak yanlış bilgilendirme, hatta kışkırtma yapılabilmektedir. Böyle durumlarda da görsele dayalı doğrulama yapmak mümkündür.

e. 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 ortamında uyulması gereken etik kurallar aşağıda verilmiştir:

- ✓ 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 sadece belirli bir ırkın, topluluğun ya da ülkenin tekelinde değildir. Tüm dünyadan pek çok farklı kültür ve inanca sahip insan İnternet ortamında varlık göstermektedir. 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.
- ✓ 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 ortamında nasıl davranılması gerektiğini öğrenmiş oldunuz. Sizin doğru davranıyor oluşunuz, herkesin de size doğru davranmasını sağlayamayabilir. İnternet ortamında başkalarından kaynaklanan kötü davranışlara maruz kalabilirsiniz. İnternet etiğine uymayan bu 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/Şikâyet Et" bağlantısını kullanarak şikâyet 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.
- ✓ Siber zorbalığa maruz kalan başka kişiler de olabilir. Böyle durumlarda bu kişilere ne yapmaları gerektiği konusunda yardımcı olabilir, kötü kullanım bildirimini siz de yapabilirsiniz. Zorba bir hesap için kötü kullanım bildirimi sayısı fazla olursa o hesabın site yönetimi tarafından incelenmesi ve kapatılması daha çabuk olacaktır.

E-Posta ve Dosya Kullanımında Kullanıcının Sorumlulukları

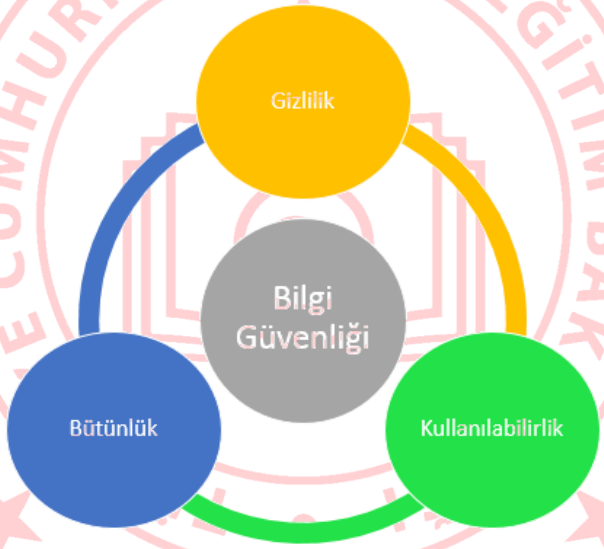
- ✓ Disk alanınızın dolmaması için, her gün e-postanızı kontrol ediniz.
- ✓ İstenmeyen mesajları diskte yer tutmaması amacıyla hemen silin.
- ✓ Posta kutunuzda bulunan mesajları minimum seviyede bulundurun.
- ✓ İlerde kullanmak için saklayacağınız mesajları, kendi bilgisayarınızın diskine kopyalayın.
- ✓ Hiçbir zaman gönderdiğiniz mesajın yalnız gönderdiğiniz kişi tarafından okunacağını düşünmeyin. Bu nedenle başkalarının eline geçince sizi zor durumda bırakacak mesajları göndermeyin.
- ✓ Bilgisayarınızı düzenli olarak virüs taramasından geçirin, özellikle başka yerlerden ve kaynağı belli olmayan yerlerden gelen dosyaları virüs taraması yapmadan kullanmayın.
- ✓ Sistem yöneticileri bilgisayarınızdaki dosyalara erişebilir. Bu nedenle diskinizde özel bilgiler bulundurmayın.

3. Bilgi Güvenliği

Bilim ve teknolojide yaşanan hızlı ilerleme, içinde bulunduğumuz yüzyılın bilgi çağı olarak isimlendirilmesine yol açmıştır. Günümüzde bilişim teknolojilerinin yaygın kullanımı ile birlikte bilginin üretilmesi ve kullanılması büyük önem kazanmış ve bu teknolojiler aracılığıyla üretilen veri miktarında da büyük bir artış olmuştur.

Bilgisayarlar ve akıllı cihazlar aracılığıyla başta internet olmak üzere bilgiye erişimin farklı yollarının ortaya çıkması da bilginin depolanması, iletilmesi ve korunması ile ilgili pek çok problemi de beraberinde getirmiştir. Bu problemlerden biri de kişisel ya da kurumsal bilgiyi erişilmez kılmaya, ele geçirmeye ya da değiştirmeye yönelik olandır.

Kişisel ya da kurumsal düzeyde 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. Bilgi güvenliği, "**gizlilik**", "**bütünlük**", "**erişilebilirlik**" olarak isimlendirilen üç temel öğeden meydana gelmektedir. Bu üç güvenlik unsurundan birinin zarar görmesi durumunda güvenlik zaafiyeti oluşabilir.



Gizlilik: Bilginin yetkisiz kişilerin eline geçmemesi için korunmasıdır. Yani bir bilgiye sadece ona erişmesini istediğimiz bir grup insanın, bazen sadece bir kişinin erişmesinin sağlanmasıdır. Bunu sağlamak bir mektubu(bilgiyi) kilitli bir kutuya koyarak göndermek ile eşdeğerdir. Kutuyu açmak için o kilidin anahtarına sahip olmak gerekeceği için, kutunun içindeki bilgiye erişim kısıtlanmış olur. (E-posta hesabınızın bir saldırgan tarafından ele geçirilmesi)

Bütünlük: Bilginin yetkisiz kişiler tarafından değiştirilmesi ya da silinmesi gibi tehditlere karşı korunması ya da bozulmasıdır. Gündelik hayatta noter kanalı ile yollanan belgelerin tahrif edilmediğinden emin olduğumuz gibi, bilgisayar ağlarında aktarılan bilgilerin de tahrif edilmediğinden emin olmak isteriz. Bunun için güncel olarak kullandığımız teknoloji ise açık anahtar alt yapısı ve sayısal imzadır. (Bir web sayfasındaki bilgilerin saldırgan tarafından değiştirilmesi)

Erişilebilirlik: Bilginin yetkili kişilerce ihtiyaç duyulduğunda ulaşılabilir ve kullanıma hazır durumda olmasıdır. Örneğin, ziyaret etmek istediğimiz kişinin kapısında bir kuyruk oluşmuşsa ve o kuyruk yüzünden onun yanına ulaşamıyorsak, o zaman erişimin engellendiğinden bahsedebiliriz. Bir çok internet sitesine dönem dönem düzenlenen ve basında adını duyduğumuz DOS saldırısı bu türde bir saldırıdır. (Bir web sayfasının saldırı sonucunda erişime kapatılması)

a. 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 adlandırılır.

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

Korsanlar ya da saldırganlar, istediklerini elde edebilmek için çok farklı teknikler kullanabilirler. Bu tür saldırı türlerinin tanınması, doğru analiz edilmesi ve gereken tedbirlerin alınabilmesi siber güvenlik için önemlidir.

Siber güvenlik: 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 Terörizm: Bilişim teknolojilerinin belirli bir politik ve sosyal amaca ulaşabilmek için hükümetleri, 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.

Bireysel saldırılarda hedefi kişisel bilgilerin ele geçirilmesi, değiştirilmesi ya da yok edilmesi oluştururken; kurumsal ve toplumsal saldırılarda ise çoğunlukla kurumların ve devletlerin zarar uğratılması hedeflenmektedir. Daha çok devletler arası düzeyde gerçekleşen siber savaşlarda ise ana hedef: sağlık, enerji, ulaşım, haberleşme gibi kritik altyapılardır.

b. Sayısal Dünyada Kimlik ve Parola Yönetimi

Her gün sıkça kullandığımız şifre ve parola kavramlarını inceleyecek olursak; parola, bir hizmete erişebilmek için gerekli olan kullanıcıya özel karakter dizisidir. Şifre ise sanal ortamdaki verilerin gizliliğini sağlamak için veriyi belirli bir algoritma kullanarak dönüştüren yapıdır.

Örneğin; e-posta hesabınıza giriş yaparken size ait olan özel karakter dizisi parolanızı oluşturmaktadır. Sanal ortamda saklanan bu parolanızın gizliliğini sağlamak için genellikle kriptografik özet fonksiyonlar kullanılmaktadır. Bu fonksiyonlar kullanılarak verilerinizin güvenliği sağlanmaktadır. Bu algoritmalardan birini kullanarak parolalarınızı şifreleyecek olursak;

Parola: 123456

Şifreleme Algoritması (md5): E10ADC3949BA59ABBE56E057F20F883E

Bir bilişim sistemine erişimin belli kurallar çerçevesinde yapılması amacıyla o sistemi kullanmak isteyen kişilerin kullanıcı adı ve parola ile erişim yetkisine sahip olduklarını ispatlamaları gerekmektedir.

Kullanıcı adı, her kullanıcıdan sadece bir tane olduğunu garantilemek amacıyla benzersiz bir bilgi olarak oluşturulur. Parola ise içinde büyük-küçük harfler, rakamlar ve özel karakterler barındıran bir karakter dizisidir.

Parola, bilgi güvenliğinin en önemli öğesidir. 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 kullanılabilir.
- 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.

Bir bilişim sistemine erişim için kanıt olarak kullanılan parolanın dikkatle belirlenmesi ve titizlikle korunması gerekmektedir. Sadece rakamlardan oluşan 6 haneli bir parolanın özel programlar yardımı ile dakikalar içinde kırılması mümkündür. Güçlü ve kırılması zor bir parolanın oluşturulması için olabildiğinde sayı, büyük/küçük harfler ile özel karakter içermesine dikkat edilmesi son derece önemlidir. Başkalarının kolaylıkla tahmin edebileceği 123456 gibi ardışık sayıların ve harflerin kullanılması, doğum yılı ya da mezuniyet tarihi gibi kişisel bilgileri içermesi zayıf parolalar için örnek gösterilebilir.

Günümüzde saldırganların parolaları ele geçirmek ya da tahmin edebilmek için sosyal medyadan faydalandıkları da unutulmamalıdır. Sosyal medya aracılığıyla ulaşılabilen aile fertlerinin adı, doğum tarihi gibi bilgiler de parola olarak kullanılmamalıdır.

Saldırganlar, sosyal medya ortamlarını kendi çıkarları için kullanarak sosyal mühendislik adı verilen ikna ve kandırma teknikleri ile bu bilgileri elde edebilir.

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 sayıla 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 hiçbir yerde saklanmamalıdır.
- ✓ Başta e-posta adresinizin parolası olmak üzere farklı bilişim sistemleri ve hizmetler için aynı parolanın kullanılmaması gerekir.

Bu durumda, bir kullanıcının onlarca parola üretmesi gerekebilir. Bu da parolaların unutulması sorununu beraberinde getirir. Böyle bir sorun yaşamamak için kullanıcılar kendilerine özgü kalıplardan yararlanmalıdır.

Örnek olarak; bir anahtar kelime belirlenerek kelime, parola kriterlerine uygun hale getirilebilir. "Masal" kelimesi, parola oluşturma kriterleri göz önüne alınarak "m@s@L" şeklinde düzenlenebilir. Bu anahtar kelimenin başına ya da sonuna kullanılan platformun kısa ismi eklenerek o hizmete özgü parola oluşturulmuş olur. Twitter için m@s@L19+Tw, Facebook için m@s@L19+Face gibi.

Anahtar kelime oluşturulurken "G" yerine "6", "Ş" yerine "$", a yerine "@" gibi karakterler kullanılabilir.

c. Kişisel Bilgisayarlarda ve Ağ Ortamında Bilgi Güvenliği

Bilgisayar ve internet teknolojisindeki hızlı ilerleme sonucunda üretilen veri, hiç durmadan artmaktadır. Özellikle internet kullanımının oluşturduğu büyük miktardaki bilgi, her gün milyonlarca insan tarafından kullanılmaktadır. Bu veriyi üreten, kullanan ve paylaşan insanların çok küçük bir kısmı ise internetin tehlikeleri ve bilgi güvenliği konusunda bilgi sahibidir. Bilişim teknolojisinin kullanımında temel amaç bilgiye erişmektir. Ancak, teknolojinin hızlı ilerleyişi ile birlikte gelen güvenlik riskleri ve insanların bu konudaki yetersiz farkındalıkları bilgisayar ve internet kullanımı sırasında pek çok tehlikenin ortaya çıkmasına neden olmaktadır.

Bilişim sistemlerinin çalışmasını bozan veya sistem içinden bilgi çalmayı amaçlayan 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 sistemine çalışarak sisteme ya da programlama zarar verme amacıyla oluşurlar. Virüsler bilgisayarlara e-posta, bellekler veya internet üzerinden bulaşabilir. Bilgisayarın yavaşlaması, programların çalışmaması, dosyaların silinmesi, bozulması ya da yeni dosyaların eklenmesi virüslerin 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.

Casus Yazılımlar: İnternetten indirilerek bilgisayara bulaşan ve gerçekte başka bir amaç ile kullanılsa bile arka planda kullanıcıya ait bilgileri de elde etmeye çalışan programlardır.

Zararlı Programlara Karşı Alınabilecek Tedbirler:

- ✓ Bilgisayara antivirüs ve internet güvenlik programları kurularak bu programların sürekli güncellenmesi gerekmektedir.
- ✓ Tanınmayan/güvenilmeyen e-postalar ve ekleri kesinlikle açılmamalıdır.
- ✓ Ekinde şüpheli bir dosya olan e-postalar açılmamalıdır.
- ✓ Zararlı içerik barındıran ya da tanınmayan web sitelerinden uzak durulmalıdır.
- ✓ Lisanssız ya da lisansı kırılmış programlar kullanılmamalıdır.
- ✓ Güvenilmeyen internet kaynaklarından dosya indirilmemelidir.