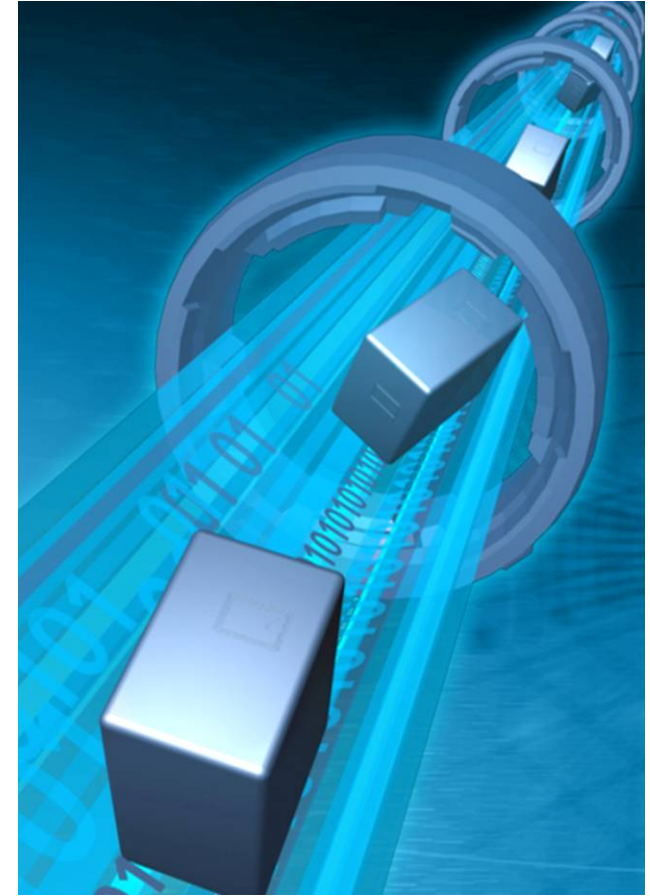


Internet ve Güvenlik

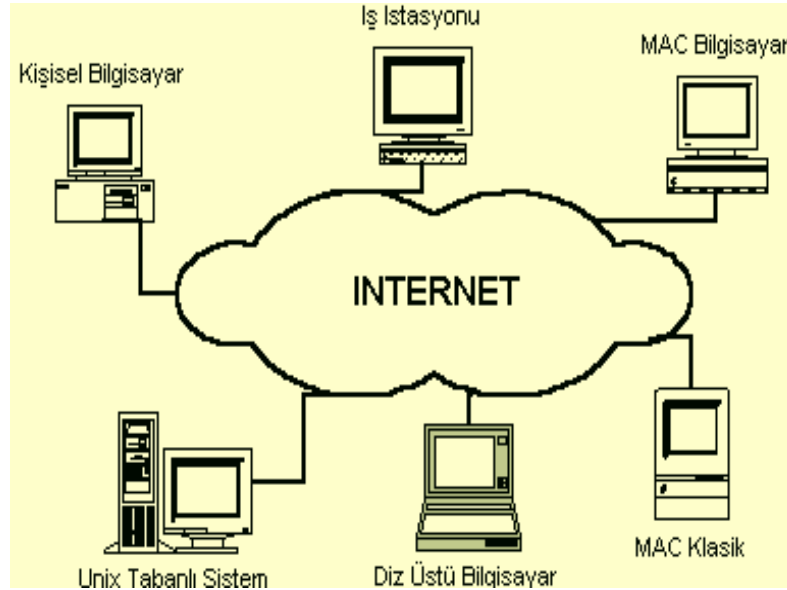
Hazırlayan ve Sunan
Yrd.Doç.Dr. Hasan H. BALIK

Giriş

- Bilgi çağı, insanlar ve kuruluşlar arasında bilgi aktarımının hızlı ve etkin olarak yapılmasını gerektirmektedir.
- Elektronik ve iletişimdeki hızlı gelişmeler dünyayı haberleşme açısından küçük bir köye (global köy) döndürmektedir.
- Kişisel bilgisayarların ve iş istasyonlarının uygun fiyatla ve kullanımı rahat programlarla ortaya çıkması yaşam biçimimizi değiştiren yeni teknolojileri ortaya çıkarmıştır.
- Gittikçe artan bir şekilde ağlar sayesinde bilgili dünya vatandaşları olarak kişisel ve toplumsal hayatı belirleyen kararlar alıp uygulayabiliyoruz.



Bilgisayar Ağları



- **Birden fazla bilgisayarın birbiriyle konuşabilecek şekilde bağlanmasına “Bilgisayar Ağı” diyoruz.**
- **Bir bilgisayar ağının görevi; yazıcı vb gibi kaynakların ve dosyaların paylaşılmasını ve ağ üzerindeki kişilerin haberleşmelerini sağlamaktır.**
- **Bir ağ üzerindeki kişiler aynı dosyayı birlikte kullanabilirler. Birbirleriyle bilgi alışverişinde bulunabilirler.**

Internet Nedir ?

- Internet sözcüğü, ingilizcede "uluslararası ağ" anlamına gelen "**inter**national **net**work" sözcüklerinin birleştirilmesinden oluşmuştur.
- Internet, bilgiye kolay, ucuz, hızlı ve güvenli ulaşmanın ve onu paylaşmanın günümüzdeki en geçerli yoludur.
- Internet, birçok bilgisayar sistemini TCP/IP protokolü ile birbirine bağlayan dünya çapında yaygın olan ve sürekli büyüyen bir iletişim ağıdır.
- Internet'in önemi, 'Olmazsa Olmaz' derecesinde sürekli olarak artmaktadır.
- 24 Ekim 1995'te FNC (Federal Networking Council) Internet'i tanıtan bir bildiri yayınladı. FNC'ye göre Internet'in tanımı aşağıdaki gibidir :
- Internet,
 - Birbirlerine, IP protokolüne dayalı global bir adres uzayı ile lojik olarak bağlı bilgisayarlardan oluşan bir bilgi sistemidir.
 - TCP/IP veya benzeri IP uyumlu protokoller kullanarak haberleşmeyi sağlar.
 - Yüksek düzeyli servislere ulaşılmasını sağlar.

Internet Nedir ?

- Dünyada bir milyardan fazla insan interneti kullanmakta ve birbirleriyle internet aracılığı ile haberleşmektedir.
- Pek çok yararlı bilginin bir tuşa basmak kadar yakın olduğu Dünya çapında dev bir kütüphanedir.
- Dünyanın en büyük, bilgisayarlı iletişim ağıdır.
- Fikirlerin serbestçe paylaşıldığı bir demokrasi platformudur.
- İnsan hayatını kolaylaştırıcı (banka, alışveriş, dergi, gazete, TV hizmetleri vb gibi) bir iletişim aracıdır.
- Çift yönlü bilgi aktarımı yapılabildiği bir haberleşme sistemidir.
- İnternet, birbirinden çok farklı donanım (PC, Macintosh,...) ve yazılım (İşletim Sistemleri:UNIX, LINUX, DOS, WINDOWS, MOS, OS/2...) özelliklere sahip olan bilgisayarların birbiriyle iletişim içinde bulunmasını sağlayan bir ortamdır.
- İnternetin tam anlamıyla bir sahibi yoktur. (kimse denetleyemez!)
- Kabaca ayda %10 oranında büyümektedir

İnternetin Tarihçesi

- İnternetin köklerini 1962 yılında J.C.R. Licklider'in Amerika'nın en büyük üniversitelerinden biri olan MIT'de tartışmaya açtığı "**Galaktik Ağ**" kavramında bulabiliriz. Licklider 1962 Ekim ayında Amerikan Askeri araştırma projesi olan İleri Savunma Araştırma Projesi'nin(DARPA-Defense Advanced Research Project Agency) bilgisayar araştırma bölümünün başına geçti. MIT'de araştırmacı olarak çalışan Lawrence Roberts ile Thomas Merrill, bilgisayarların ilk kez birbirleri ile 'konuşmasını' ise 1965 yılında gerçekleştirdi.
- 1966 yılı sonunda Roberts DARPA'da çalışmaya başladı ve "ARPANET" isimli projesi önerisini yaptı. ARPANET çerçevesinde ilk bağlantı 1969 yılında dört merkezle yapıldı ve ana bilgisayarlar arası bağlantılar ile internetin ilk şekli ortaya çıktı.
- Kısa süre içerisinde birçok merkezdeki bilgisayarlar ARPANET ağına bağlandı.
- 1 Ocak 1983 tarihinde İletişim Kontrol Protokolü (Transmission Control Protokol/ internet protokol - TCP/IP) adıyla ARPANET içinde kullanılmaya başladı. TCP/IP bugün varolan internet ağının ana halkası olarak yerini aldı.
- 1980 yılların ortasında Savunma Bakanlığı'na bağlı (DoD) Amerikan askeri bilgisayar ağı, ARPANET'ten ayrıldı ve MILITARY NET adı ile kendi ağını kurdu. 1986 yılında Amerikan bilimsel araştırma kurumu 'Ulusal Bilim Kuruluşu' (NSF), ARPANET için ülke çapında beş büyük süper bilgisayar merkezi kurulmasını içeren kapsamlı bir öneri paketi öne sürdü. ARPANET Amerikan hükümetinin sübvansiyonu ile NSFNET olarak düzenlendi. 1987 yılında yeniden düzenlediği internet yapılanması planı ile NSFNET yedi bölgesel nokta üzerinde 1.5 Mb/s (daha önce 56 Kb/s idi) güçlü bir omurgayı işleteceğini duyurdu.

Internetin Tarihçesi

- NSFNET'in işletilmesine yönelik 1990 yılında oluşturulan birlik 'İleri Ağ Hizmetleri' (ANS-Advance Network Services) olarak adlandırıldı. ANS'nin kuruluşu süreci ABD'de 1990'lara kadar devlet desteğinde gelişen internet omurgasının özelleştirilmesi sürecinin de başlangıcı olmuştur.
- 1990 yılında NSFnet ile özel şirketlerin ortak işletmesi ile başlayan özelleştirme süreci, 1995 yılı mayıs ayında NSF'nin internet omurga işletmeciliğinden tamamen çekilmesi ile tamamlandı. 1995 yılından itibaren ABD internet omurga işletimi tamamen özel işleticilerinin elindedir.
- İnternet'e çeşitli şekillerde, başlangıcından 1994 yılı sonuna kadar 110 ülke, 10,000 bilgisayar ağı, 3,000,000 dan fazla bilgisayar ve 25 milyonu aşkın kullanıcı bağlanmıştır. Bu sayı, Web Sayfası kavramının kullanıma girdiği 1995 yılı içinde büyük bir patlama göstermiş ve 60 milyon'a ulaşmıştır. Bu sayının 1996 yılı içinde de, her ay yüzde 10 artması beklenmekteydi. Ve şu an Türkiye' de 5 Milyon, Dünyada toplam 300 Milyon İnternet kullanıcısı olduğu sanılıyor. Görüldüğü üzere İnternet büyük bir hızla dünyanın her köşesine din, dil, ırk ve ülke ayrımı yapmadan erişmektedir. Şu an yeni yüzyılın en büyük iletişim ve reklam araçlarının başında gelmektedir.

TCP/IP Nedir ?

- "Bilgi Ağı" üzerindeki bilgi iletimi ve paylaşımı bazı kurallar dahilinde yapılmaktadır. Bu kurallara kısaca "internet protokolleri", ya da TCP/IP protokoller ailesi denir.
- TCP/IP (Transmission Control Protocol / Internet Protocol), bilgisayarlar ile veri iletme/alma birimleri arasında organizasyonu sağlayan, böylece bir yerden diğerine veri iletişimini olanaklı kılan pek çok veri iletişim protokolüne verilen genel addır.
- Bir başka deyişle, TCP/IP protokolleri bilgisayarlar arası veri iletişiminin kurallarını koyar.
- Bu protokollere örnek olarak, dosya alma/gönderme protokolü (FTP, File Transfer Protocol), Elektronik posta iletişim protokolü (SMTP Simple MailTransfer Protocol),TELNET protokolü (Internet üzerindeki başka bir bilgisayarda etkileşimli çalışma için geliştirilen login protokolü) verilebilir.
- TCP/IP'nin bir parçası olan ve adını sıkça duyduğumuz WWW ortamında, birbirine link objelerin iletilmesini sağlayan protokol ise Hyper Text Transfer Protocol (HTTP) olarak adlandırılmaktadır.
- TCP/IP protokol kümesi aynı zamanda, diğer iletişim ağlarında da kullanılabilir. Özellikle pek çok farklı tipte bilgisayarı veya iş istasyonlarını birbirine bağlayan yerel ağlarda (LAN) kullanımı yaygındır.

Internet Neyi Sunar ?

- Internet, teknik olarak, TCP/IP protokolü ile desteklenen pek çok servis sunar. Örnek olarak, Internet erişimi olan bir kullanıcı, eğer kendisine yetki verilmişse, Internet' e bağlı diğer herhangi bir bilgisayardaki bilgilere erişebilir, onları kendi bilgisayarına alabilir, kendi bilgisayarından da Internet erişimi olan başka bir bilgisayara dosya/bilgi gönderebilir. Bu özellik, dosya transfer protokolü olarak bilinir.
- İçerik bakımından ise, Internet' in sundukları bazen insan hayal gücünü zorlayacak boyutlara varmaktadır. Vizyondaki filmlerin kısa tanıtımlarını kolayca evimizdeki ekrana taşıyabilir ya da Amerikan Kongre Kütüphanesi'nde tarama yapabiliriz, TÜBİTAK arşivine bağlanıp Bilim ve Teknik dergilerinin yeni ve eski sayılarını tarayabilir, yazıları okuyabiliriz, Hacettepe Üniversitesi'ne uzanıp o anki Beytepe Kampüsü sıcaklıklarını grafiksel olarak görebiliriz, katılmak istediğimiz bir bilimsel toplantıya bildirimizi Internet üzerinden gönderebiliriz. Örnekleri arttırmak mümkün; NASA servislerine bağlanıp, son uydu fotoğraflarını tarayabiliriz, şiir arşivlerine bağlanıp şiirler okuyabiliriz. Son yıllarda geliştirilen www ve (yavaş yavaş unutulmasına rağmen, o bir klasikti) Gopher gibi modern Internet araçları ile bilgiye ulaşım daha da kolaylaşmış, ulaşılacak bilgiler ve sunulan servisler miktar ve çeşit olarak artmışlardır.
- Internet' in sundukları; onu kullananların istekleri, hayal güçleri ve gelişen Internet teknolojisi ile hep artmaktadır.
- Internet, bilgiye ulaşmayı kolaylaştırmak için değişik 'bilgi tarama' yöntemleri de sunar.
- Internet' in sundukları çok geniş ve bu kadar bilgi arasında, bilinçsiz bir kullanımla, insan yolunu çok kolay kaybedebilir.

İnternete Bağlanma

- İnternet' e kişisel bağlantı için bir bilgisayara, bir modeme, bir telefon bağlantısına ve servis sağlayıcıdan alınmış kullanıcı şifresine gereksinim vardır.
- **Modem Nedir?**
 - Bir bilgisayardan diğer bir bilgisayara iletilecek olan bilgiyi telefon kablolarından geçebilecek duruma dönüştürür, bilgisayara diğer bir bilgisayardan gelen bilgileri de bilgisayarın anlayabileceği duruma getirir.
 - Modemler hızlarına göre sınıflandırılır. Modemlerin veri iletişim hızları "bps" (bit per second) olarak ifade edilir. Bu da modemin saniyede kaç bit taşıdığı anlamına gelir. 57600 bps veya 512 kbps gibi. Hızlı modem, bilgiye kısa zamanda ulaşmayı sağlayan unsurlardan bir tanesidir.
 - Bilgisayar kasasının içinde olan modemlere dahili (internal), kasanın dışında olan modemlere de harici (external) modemler adı verilir. Modemin kasanın içinde ya da dışında olması modemlerin işlevini etkilemez ya da değiştirmez.
- **Servis Sağlayıcı Nedir? (Internet Service Provider (ISP))**
 - İnternet' e bağlanmayı sağlayan aracı kuruma servis sağlayıcı denir.
 - İnternet' e bağlanmak için servis sağlayıcı kurumdan kullanıcı şifresi ve bağlantı için kullanılacak telefon numarası alınır. Bağlantı kurulduğunda servis sağlayıcı, bilgisayar için geçici bir IP adresi belirler. Farklı bağlantılarda IP adresi değişerek İnternet'e bağlantı yeni bir IP adresi ile sağlanır.
 - Servis sağlayıcının hat kapasitesi, İnternet' e bağlanma hızını etkiler. Seçiminizi yaparken servis sağlayıcıların hat kapasitelerini öğrenip, en yüksek olanını seçmeniz İnternet' e bağlantı hızınızı olumlu yönde etkileyecektir.

DSL ve ADSL

■ DSL nedir?

- DSL (Digital Subscriber Line – Sayısal Abone Hattı) teknolojisi, standart bakır kablolar aracılığıyla yüksek bant genişliği sunan bir veri iletimi teknolojisidir.
- DSL teknolojisi, şu anda bütün dünyada yaygın olarak sıradan telefon hatları aracılığıyla kullanılmaktadır.
- Sayısal kodlama tekniği ile mevcut telefon hattının bandı artırılarak daha verimli şekilde kullanılabilmesi sağlanmaktadır.

■ DSL teknolojisinin avantajlı yönleri

- Dünya üzerinde mevcut durumda kurulu olan telefon hattı hemen hemen tüm gerekli noktalara ulaşabilmektedir ve ek bir tesisat çekilmesi zorunluluğu yoktur. Böylece ekstra altyapı maliyeti doğmamaktadır.
- Aynı telefon hattı üzerinden hem ses / faks hem de internet verisi gönderebilir. Bu sayede çevirmeli bağlantının aksine internet bağlantısı devam ediyor olsa da aynı hat üzerinden telefon görüşmesi de yapılabilir. Böylece aynı anda telefon görüşmesi de yapmak isteyenler için yeni bir telefon hattı gerekliliği doğmaz.
- Sağlanan internet erişimi kesintisizdir ve yüksek hızlarda download/upload imkanı mümkündür. Yani bilgisayarınız açık olduğu sürece internete bağlı olmamız için herhangi bir neden yok. En hızlı analog modem ile elde edilebilecek hızdan 200 defa daha hızlı erişim sağlamak olasıdır.
- İlk yatırım düşüktür. Kullanıcılar için DSL modem dışında başka bir cihaz gerektirmez. Servis sunan firmalar içinse, santrale kurulacak cihaz alınması gereklidir.
- Kesintisiz ve hız dalgalanması yaratmayan DSL, düşük ping süreleri sayesinde online oyunlar için son derece uygundur.
- Bağlantı kopması ve yoğun saatlerde hız kaybı gibi sorunlar yoktur.

xDSL ailesi ve üyeleri

- DSL teknoloji ailesinin HDSL, VDSL, ADSL ve bunların türevleri gibi pek çok çeşidi bulunmaktadır.
- Bu yüzden bu ailenin hepsini birden ifade eden xDSL terimi kullanılır. Buradaki x karakteri, farklı DSL bağlantı tipleri için ilk harfin değiştiğini ifade ediyor.
- Bu bağlantı tiplerinden bazıları sadece teoride kalmış olsa da bazıları yaygın şekilde kullanılmaktadır. Aşağıda yer alan tabloda görüldüğü gibi farklı türler arasında bant genişliği ve santrale olan uzaklıklar önemli rol oynar.
- Bunlar içinden en yaygın şekilde kullanılan DSL ailesi üyesi ADSL ve SDSL'dir.

Türü	Anlamı	Maksimum bant Genişliği (Download/Upload)	Santrale Uzaklık Snr
IDSL	ISDN Digital Subscriber Line	128 Kbps/128 Kbps	5.4 km
ADSL Lite	Splitterless DSL	6Mbps/2.048 Mbps	3 km
HDSL	High bit-rate Digital Subscriber Line	1.544Mbps/2.048 Mbps	3 km
SDSL	Symmetric DSL	2 Mbps/2 Mbps	3 km
ADSL	Asymmetric Digital Subscriber Line	8.4 Mbps/640Kbps	2.7 km
VDSL	Very High Digital	52.8 Mbps/2.3 Mbps	250 m

ADSL

- XDSL ailesi içinde en çok tercih edilen üye olan ADSL(Asymmetric Digital Subscriber Line=Asimetrik Sayısal Abone Hattı)'nın adında yer alan asimetrik ifadesi downstream ve upstream veri iletiminin eşit olmadığını ifade etmektedir.
- Örneğin, bugün için ülkemizde sunulan en düşük ADSL bağlantı tipi olan 512/128 tipinde, teorik olarak 512 Kbps hızında download ve 128 Kbps hızında upload imkanı bulunur.
- Ev tipi kullanıcılar için download kapasitesi daha önemli olduğu için ADSL bağlantının getirdiği herhangi bir dezavantaj yoktur. Ayrıca verimsiz şekilde kullanılacak upload bant genişliği tahsis edilmediğinden toplam bant genişliği daha verimli şekilde paylaştırabilmektedir.

Ülkemizde ADSL ve Internet

- ADSL, şu anda en popüler Internet servisi olup 1.5 milyondan fazla abonesi vardır.
- Abone sayısı son bir yılda %237 artış göstermiştir.
- 1.Ocak.2006 itibarı ile Ortadoğu ve Afrika bölgesinde ADSL abone sayısı 1 milyonu geçen tek ülke Türkiye'dir.
- Türkiye bu büyüme rakamı ile dünyada ADSL ye en hızlı geçiş yapan 2. ülke konumundadır.
- ADSL abone sayısı itibarı ile dünyada 16. sıradadır.
- Ülkemizde telefon hatlarının %8.2 lik trafiği ADSL için kullanılmaktadır.

ADSL mi? Dial-Up mı?

Hangisini seçmeli?

- Bağlantı hızı ve bant genişliği açısından çevirmeli bağlantı (Dial-Up Modem) ve ADSL'i karşılaştırmak gerektiğinde ADSL hizmetinin avantajlı olduğu kolaylıkla görülebilir.
- Ülkemizdeki ADSL hizmeti giriş seviye üyelikte bile 512/128 Kbps hızına sahiptir. Bu yüzden teorik download hızı, çevirmeli ağı sağladığı 56 Kbps değerinin 10 katına yakındır.
- Diğer yandan ADSL de bağlantının hiç kesilmiyor olması ve telefon hattını meşgul etmemesi, hem telefon için hem de servis sağlayıcı için para ödeme gerekliliğinin olmaması ADSL'in diğer avantajlarıdır.
- Her gün sadece bir saat internete girip belirli siteleri gezen bir kullanıcı için ADSL'in ekonomik olmadığını da belirtmek gerekir.
- Çevirmeli bağlantıda kullanılan analog modemlerin fiyatları ADSL modemlere nazaran 3 ila 10 kat arası daha ucuzdur.
- Ayrıca çevirmeli bağlantı aracılığıyla telefon olan herhangi bir noktadan pek çok farklı internet servis sağlayıcı arasından isteğe bağlı seçim yaparak internete bağlanabilme olanağı bulunmaktadır.

Internet Adresleri

- Internet' e bağlı her bilgisayarın kendine özgü bir adresi vardır.
- Internet adresleri, insanları, bilgisayarları ve Internet kaynaklarını tek olarak tanımlamak için kullanılırlar.
- Internet adresleri aşağıdaki gibi ele alınabilir;
 - IP (Internet Protokolü) adresleri
 - Domain (alan) adları.
 - E-mail (Elektronik Posta) adresleri.
 - URL'ler.

IP Adresleri

- Internet'te her bilgisayarın bir IP (Internet Protokol) adresi vardır.
- IP adresi, TCP/IP standardını kullanan bir ağdaki cihazların birbirini tanımak, birbirleriyle iletişim kurmak ve veri alışverişinde bulunmak için kullandıkları benzersiz bir numaradır.
- Internet bağlantısı bulunan her cihazın bu cihaza tahsis edilen bir adresi olması gerekir. Bu adres, iletilen bilginin doğru adrese gönderilmesini, ya da verinin doğru adresten alınmasını sağlar.
- Hiyerarşik bir dağılıma sahip değildir. Yani ardarda gelen iki IP adresi dünyanın çok farklı iki coğrafyasında bulunabilir.
- Bugün halen kullanılmakta ve test edilmekte olan iki tür Internet Protokolü vardır: IPv4 ve IPv6.

IP Adresleri

■ IPv4

- Bu, halen kullanılmakta olan standart Internet protokolüdür ve **32 bitten** oluşur.
- Tipik bir IP adresi, noktalarla ayrılan dört sayı ile gösterilir. Buna Noktalı Onluk Gösterim (Dotted Decimal Notation) denir.
- Bu sayılar, 0 ila 255 arasında değişir. Örneğin **193.255.124.6** gibi.
- IPv4 protokolündeki bir adres 0.0.0.0 ila 255.255.255.255 arasında herhangi bir numara olabilir.
- Bu adreslerde Net ve Host şeklinde iki kısım vardır. Net kısmının büyüklüğüne göre A,B,C,D gibi sınıf (class) lar mevcuttur.
- Bu protokol kullanılarak **4 milyardan fazla** adres üretilebilmektedir.

■ IPv6

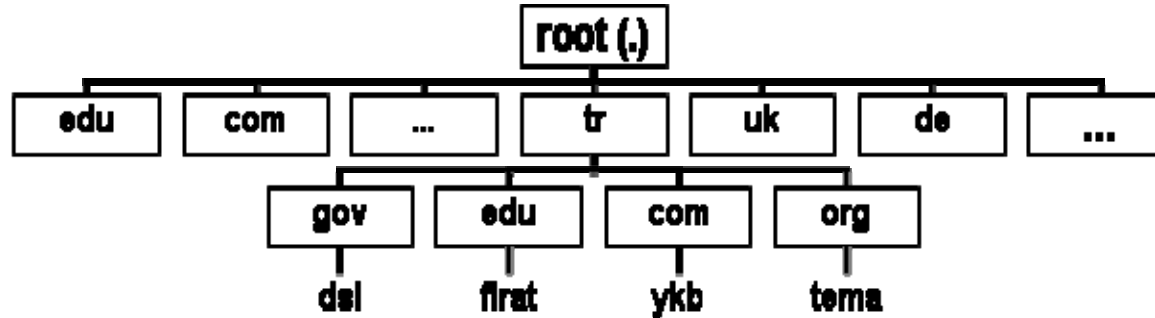
- IP adreslerinin bloklar halinde tahsis edilmesi nedeniyle, birçok IP adres aralığı kullanılamamaktadır, bu nedenle artan ağ kullanıcısı sayısına bağlı olarak, daha büyük bir IP adresine ihtiyaç duyulmaktadır. IPv6 bu ihtiyaçtan doğmuştur.
- IPv4'ten farklı olarak IPv6, 128 bit genişliğindedir, bu da 2^{128} adet, başka bir ifadeyle 3×10^{38} adet benzersiz adres demektir.
- IPv6 ile dünya üzerindeki her M^2 ye **655.570.793.348.866.943.898.599 = 6.5×10^{23}** IP düşmektedir.

IP adresi ne işe yarar?

- IP adresi ya da numarası, bugün suçluların takibinden online satış ve pazarlamaya kadar çok çeşitli alanlarda yaygın olarak yararlanılan bir veridir.
- IP numarasına bakarak kullanıcının bulunduğu ülkeyi, kenti, enlem ve boylamı ve ISS'yi (İnternet Servis Sağlayıcısı) belirlemek mümkündür.
- Bu amaçla on binlerce IP numarasının bulunduğu büyük veritabanlarına ve IP numarasına denk düşen ülke, kent, ISS gibi verileri alacak program koduna ihtiyaç duyulmaktadır.
 - Sayfanın, ziyaretçinin ana dilinde ve para biriminde gösterilmesi
 - Ziyaretçilerin, coğrafi bölgeye göre farklı sayfalara yönlendirilmesi
 - Sayısal hakların yönetimi
 - Şifre paylaşımının ve hizmet istismarının önlenmesi
 - Kredi kartı dolandırıcılığının önlenmesi
 - İnternet ziyaretçi trafiği istatistiği ve analizi
 - Online formlarda ülkeyle ilgili formun otomatik olarak seçilmesi
 - İş yapmak istemediğiniz ülkelerden erişimin engellenmesi
 - Satışların ve bağlantı tıklama oranının artırılması için coğrafi hedefleme (geo targeting)
- Bugün dünyada, bu tür büyük veritabanları oluşturan ve düzenli olarak güncelleyen firmalar mevcuttur.

Alan Adları ve DNS (Domain Name System)

- Bir IP adrese sahip olan herhangi bir cihaza bir isim atanabilir.
- İsimlere ihtiyaç duyulmasının nedeni, sayısal İnternet adreslerine kıyasla daha kolay hatırlanabilir olmalarıdır. Çoğu zaman alan isimleri ve IP adresler, birbirinin yerine kullanılabilir.
- Alan adları, hiyerarşik bir yapıda düzenlenmiştir. Hiyerarşinin en belirgin elemanından, en az belirgin elemanına kadar yazılıp araya birer nokta konulmasıyla Tam Tanımlanmış Alan Adı (FQDN - Fully Qualified Domain Name) elde edilir.
- “DNS” alan isimleri ile IP adresleri arasında eşleştirmeler yapan dağıtık bir veritabanı sistemidir.
- DNS sunucu verilen bir makina adının IP adresini çözerek makinaların İnternet üzerinde alan isimleri ile haberleşmelerine olanak tanır. Bu ayrık veritabanı sistemi İnternet’in başarısında büyük bir rol oynar. İnternet üzerinde makina isimlerinin dağıtılması bir makina üzerine gelebilecek fazla yükü alır. Tek bir kişinin veya kurumun İnternet isimlerini İnternet’in büyüme hızına paralel olarak tutabilmesi imkansızdır. İnternet komitesi bu sorunu Domain Naming Sistemi (DNS) kurarak çözmektedir.



gov : Hükümet kuruluşları, **edu** : Eğitim kurumları (üniversiteler gibi), **org** : Ticari olmayan, kar amacı gütmeyen kuruluşlar, **com** : Ticari kuruluşlar, **mil** : Askeri kuruluşlar, **net** : Servis Sunucuları (İnternet Servis Sağlayıcıları gibi), **ac** : Akademik kuruluşlar (bazı ülkelerde edu yerine kullanılmaktadır.), **int** : Uluslararası organizasyonlar, kuruluşlar

E-mail (Elektronik Posta) adresleri

- Birisine bir mektup gönderdiğinizize göre bu mektubun gideceği bir geçerli adres olmalıdır. Elektronik ortamda bu adres, “e-mail (e-posta) adresi” olarak adlandırılır.
- E-posta adresi, genellikle, kişinin kullanıcı adı ve kullandığı sistemin Internet adresinden oluşur.
- info@hasanbalik.com veya hasanbalik@gmail.com örnek e-mail adresleridir.
- Dikkat edilirse adres, @ işareti ile ayrılmış iki kısımdan oluşur. İlk kısım kişinin kendi sistemindeki kullanıcı adı; ikinci kısım ise, bulunduğu sistemin adresini belirtir.
- Bazı sistemler, ilk kısımdaki kullanıcı adı yerine başka isimlere de izin verir. Bazı farklı ağlarda (CompuServe, UUCP gibi) daha değişik e-posta adresleme formatları vardır.

URL (Unform Resource Locators)

- URL (Unform Resource Locators) yada diğer adıyla Link, Web Browser'lar içinden bir Web servisine ya da diğer bazı Internet servislerine yönlendirme yapılabilmesini sağlayan bir komut formatıdır. URL'ler bir bakıma, Internet üzerinde erişebileceğimiz servisleri belirtmek, tanımlamak için kullandığımız adreslerdir.
- Web Browser içinden 'Open URL' ya da 'Open Location' şeklinde bir seçenek üzerinden uygun URL satırları verilerek, Web, FTP, news, gopher, wais, telnet erişimi yapılabilir. unix için lynx kullanarak, bu URL'ler bir parametre gibi verilir (lynx <URL satırı>) ya da ilk sayfadan GO seçilir.
- URL satırlarının genel formatı :

<servis>://<adres>[:port_numarası]/<dizin>/dosya_adı

- şeklindedir. <servis> yerine web için http, FTP için ftp, telnet için telnet, gopher için gopher, wais için wais, haber grupları için news yazılmalıdır.
- Aşağıda bazı örnek kullanımlar gösterilmiştir.
 - Web Erişimi : <http://www.tubitak.gov.tr/form/index.html> veya <http://www.hasanbalik.com>
 - Gopher : <gopher://gopher.bilkent.edu.tr>
 - News : <news://comps.os.linux>
 - FTP : <ftp://ftp.metu.edu.tr/>

World Wide Web (www) Nedir?

- WWW, Web, ya da W3 (World Wide Web), yazı, resim, ses, film, animasyon gibi pek çok farklı yapıdaki verilere kompakt ve etkileşimli bir şekilde ulaşmamızı sağlayan bir çoklu hiper ortam sistemidir.
- Hiper ortam, bir dökümandan başka bir dökümanın çağırılmasına (navigate) olanak sağlar (iç içe dökümanlar). Bu ortamdaki her veri (object), başka bir veriyi çağırabilir (link). Link, aynı döküman içinde başka bir yere olabildiği gibi, fiziksel olarak başka bir yerde (internet üzerindeki herhangi bir makinada) de olabilir. Bütün bu farklı yapıdaki veriler uygun bir standart ile bir arada kullanılıp bir Web Listeleyicisinde (Web Browser) görüntülenebilir.
- Web'in diğer bir işlevi de, öteki bazı internet servislerini kendi içerisinde barındırmasıdır (ftp, gopher, news, wais gibi).
- Web uygulamaları (Web sayfaları), Web Listeleyicilerinde (Browser, Gezgin, Tarayıcı) görüntülenir. Web sayfaları, başka sayfalara ve değişik türden verilere hiper linkler içermektedir. Buralara fare ile tıklayarak, başka sayfalara, oradan da başka sayfalara geçeriz. Bu aslında çok basit bir bilgiye ulaşım modelidir.

World Wide Web (www) Nedir?

- Web Sistemleri, kullanılan platformdan bağımsızdır. Bir Macintosh, Pc ya da Unix Web Listeleyicisi aynı sayfaları, aynı şekilde alırlar.
- Web yapısının bu kadar çok kabul görmesinin bazı sebeplerini sıralamak gerekirse :
 - Her şeyden önce Web, açık bir sistemdir. Platform, bilgisayar, işletim sistemi vb. bir bağımlılığı yoktur.
 - Web üzerinden pek çok bilgi kaynağına kolayca erişilebilir.
 - Web uygulamaları geliştirmek ve bunları kullanıma sunmak çok kolaydır. Çoğu durumda, uzmanlık gerektirmez ve fazla bilgisi olmayan birisi bile Web sayfaları dizayn edip kullanıma sunabilir.
 - Aranılan bilgilere, birtakım tarama mekanizmaları (Search Engines) sayesinde kolayca ulaşılabilir.
- 1996'dan sonra, Web'in başka bir işlevi daha ortaya çıkmıştır. Web aslında bir işletim sistemi!! Şeklinde de tanımlanabilir. Başka bir deyişle birbirine bağlı bilgisayarlar arasında veri paylaşımı için kuralları olan, iyi bir grafik ara birimli bir işletim sistemi. Şu an bile, Web arayüzü ile, sabit diskimizdeki dosyalar arasında gezinebiliriz. Tıpkı, başka bilgisayarlardaki sayfalar arasında gezindiğimiz gibi. Günümüzde Web arayüzlü işletim sistemleri konusunda ciddi araştırmalar vardır.

Web'in Kısa Tarihi

- Web, ilk olarak, Mart 1989'da, "Yüksek Enerji Fiziği" konusunda dünyanın değişik kesimlerinde araştırmalar yapan kişiler arasında etkin ve kolay bir haberleşme platformu olarak Tim Berners-Lee tarafından CERN'de (European Particle Physics Laboratory) geliştirilmeye başlanmıştır.
- 1991 yılında da kullanılmaya başlanmıştır. 1992'de "line mode" çalışan bir Web listeyici (WWW Browser) dağıtılmaya başlanmıştır. Ocak 1993'te tüm dünyada 50 tane Web sitesi servis vermekteydi. 1993, Web için bir çok dönüm noktalarını içermektedir. Şubat 1993'te, X-Windows için Mosaic'in ilk alfa sürümü NCSA'da Marc Andreessen tarafından geliştirilerek bedava kullanıma sunulmuştur.
- Mart 1993'te, tüm Internet trafiğinin %0.1'i Web tarafından oluşturulmaktaydı. Ekim 1993'te dünyadaki Web sitesi sayısı 500'e, oluşturulan trafikte %1 mertebelerine çıkmıştır.
- Aynı yıl içinde, ilk zamanlarda çok popüler olan bir başka Web listeyici: Cello da piyasaya sürülmüştür. 1994 yılı, standartların oturması ve Web browserlerin birbiri peşisıra çıktıkları bir yıldır. İlk Web konferansı bu yıl içinde Cenevre'de düzenlenmiştir. Mosaic'i geliştiren grup, "Netscape Communications Corporation" adında ayrı bir oluşum altında şu an en çok kullanılan Web listeyici olan "Netscape Navigator" 'ın ilk beta (0.9) sürümünü Kasım 1994'te pek çok platform için (windows, mac, unix) çıkarmıştır.
- Yine 1994 içinde, CERN ve MIT (Massachusetts Institute of Technology) arasında varılan bir anlaşma ile ortak bir grup oluşturulmuştur: W3 Organization (<http://www.w3.org>). Bu grup, Web ile ilgili her türlü gelişimi yönlendirmek amacıyla oluşturulmuştur. 1995 yılında bu grup, W3 Consortium adını almıştır.
- Günümüzde ise Web, Internet'in kalbi gibidir.

HTTP

(Hyper Text Transfer Protocol)

- WWW, http (Hyper Text Transfer Protocol) adı verilen protokolü kullanarak web sayfalarını görüntüler.
- Http bir anlamda internet ağı üzerindeki iletişim dilidir.
- Bir Web dökümanına ulaştığımızda her şey 4 ana fazda gerçekleşir:
 - Bağlantı,
 - Ne istediğimizin Web servisine iletilmesi,
 - Cevap,
 - İlgili sayfaya yapılan bağlantının kesilmesi.
- Bu ana safhalar, Web üzerinde iletişimin kurallarını tanımlayan bir protokolü oluştururlar. Bu protokole de, Hyper Text Transfer Protocol (HTTP) denir.
- Bağlantı safhasında, Web erişiminde kullanılan bir Web listeleyici (browser, Web client), ilgili bilginin olduğu Web servisine bağlanır. Bu servislere HTTP servisleri de denir.
- Bağlantı sağlandıktan sonra Web istemci programımız http servisine “ne istediğini” bildirir. Bu “istek”, “http”, “ftp”, “e-mail” gibi bazı protokol kurallarını içerir ve bu işlemlere genel olarak “navigate” de denir.
- Bu isteği alan http servisi de, istediğimiz işlemi yapar ve cevabı bize gönderir. Biz de gelen cevabı Web istemci programımızda görürüz.
- Eğer istek gerçekleştirilemiyorsa bir hata mesajı ile karşılaşırız. Son safhada ise, http servisine yaptığımız bağlantı kesilir.

HTML

(Hyper Text Markup Language)

- HTML, ana hatları SGML (Standard Generalized Markup Language) ile belirlenmiş bir döküman formatlama dilidir. Bu dil, daha çok, yazılı bir dökümanı formatlamak ve bir objeden başka bir objeye linkler sağlamak ile ilgili komutlar içerir.
- Son yıllarda, HTML içinde, salt döküman formatlama dışında işler yapan CGI, Java, JavaScript gibi unsurlar da kullanılmaktadır. Ayrıca, 2.0'dan sonraki sürümlerde, tablo kullanımı, doldurulabilir form kullanımı, frame vb gibi pek çok yenilik göze çarpmaktadır.
- İnternet üzerinde görmüş olduğunuz web dosyalarının uzantıları genel olarak htm veya html (Hyper Text Markup Language) dir.
- HTML aynı zamanda web sayfaları hazırlamak için kullanılan kodlardır.
- HTML statik bir yapıya sahiptir. Özellikle her gelen isteğe farklı şekillerde cevap verilmesi gereken durumlarda yetersiz kalır. Bu durum web programcıları için zamanla yeterli olmamış ve (Javascript, Vbscript gibi bazı) script dilleri geliştirilmiştir bunlarda HTML kodlarının içerisine yerleştirilebilmekle beraber gelen isteğe göre html sayfalarının dinamik olarak oluşturulmasına olanak sağlarlar. Bu tarz script dilleri genelde iki kategoriye ayrılır.
 - Sunucu Taraflı (Server Side)
 - İstemci Taraflı (Client Side)
- ASP (Active Server Pages), CGI, PHP gibi diller Server tabanlı dillerdir. Bunlar web sunucular üzerine koşarlar ve çok daha dinamik ve kullanışlı web sayfaları hazırlanmasını sağlarlar.
- Öte yandan JavaScript gibi diller ise istemci tarafında çalışırlar ve daha çok istemci tarafında gerekli kontroller ve dinamik yapı oluşturmada kullanılır.

Arama Motorları

(Internet'te istenilen bilgiyi bulma)

- Günümüzde, Internet'in en popüler uygulamalarından biri olan www üzerinde bilgi içeren yaklaşık bir trilyona yakın belge olduğu ve bu belgelerin her yıl 2-3 katına çıktığı tahmin edilmektedir.
- Aradığımız her türlü bilgiye sadece birkaç tuşla ulaşmak mümkün olsa da Internet kullanıcıları ihtiyaç duyduğu anda bilgiye erişebilmek için o bilgiyi içeren belgenin web adresini bilmek zorundadır.
- Hergün Web ortamına eklenen milyonlarca yeni belgenin yanında mevcut milyonlarca belge de siliniyor ya da değiştiriliyor. İşte bu noktada Internet kullanıcılarının aradığı bilgiye ulaşmalarını sağlamak amacı taşıyan ve dinamik bir rehber görevini gören arama motorları devreye girmektedir.
- Arama motorları, kullanıcıların ulaşmak istediği bilgi ile ilgili girmiş olduğu bir veya birden fazla sözcüğü kendi dinamik veri deposunda tarayıp kullanıcıya aradığı bilgiyi içerebilecek ilgili belgeleri listelemektedir.
- Arama motorları hiç durmaksızın Web üzerindeki siteleri ziyaret etmekte ve bu sitelerin içeriği hakkında bilgi toplamaktadırlar. Ayrıca önceden ziyaret ettikleri sitelerin hala aktif olup olmadıklarını, içeriklerinin değişip değişmediğini de kontrol ederler.
- Kısaca sürekli değişen Web üzerindeki belgeler hakkında bilgi toplamakta ve daha sonra kullanıcıların girdiği birkaç kelime karşılığında, ilgili olabilecek belgeleri önceden oluşturduğu veri deposundan elde edip en ilgiliden en ilgisize doğru sıralı bir şekilde kullanıcılara listelemektedirler.

Arama Motorları

(Internet'te istenilen bilgiyi bulma)

- Diğer bir deyişle; Arama motorları, Internet üzerindeki web sitelerini, başlıklarına, açıklamalarına, anahtar kelimelerine ve içeriklerine göre indeksleyen sistemlerdir.
- Webde çokça bilinen arama motorlarına örnek;
 - Google (<http://www.google.com>),
 - Yahoo (<http://www.yahoo.com>),
 - MSN (<http://www.msn.com>),
 - Altavista (<http://www.altavista.com>),
 - Excite (<http://www.excite.com>),
 - Lycos (<http://www.lycos.com>),
 - HotBot (<http://www.hotbot.com>).
- Bunun yanında Türk arama motorlarına bir kaç örnek verirsek;
 - Dizin (<http://www.dizin.cc>),
 - AraBul (<http://www.arabul.com>),
 - HemenBul (<http://www.hemenbul.com>),
 - NetBul (<http://www.netbul.com>) vb.

Web Kullanımı ile İlgili Akılda Tutulması Gerekenler

- Rastladığınız ilginç siteleri “Bookmark” etmeyi unutmayın. Sonradan ziyaret etmek istediğinizde bulmanız çok kolay olur.
- Kullandığınız Web Listeleyicisinin yeteneklerini iyi öğrenmeye çalışın. Pek çok Web listeleyicisinde, hazır site grup adreslerine (Konu katalogları) doğrudan menülerden erişilebilir. Ayrıca, ziyaret ettiğiniz sayfaların HTML kodlarını Web listeleyicinizle görebilme şansınız var. Bu da önemli bir araç.
- Bir web Arama/Tarama servisinin kullanımını iyice öğrenin.
- Ziyaret ettiğiniz sayfalardaki hoşunuza giden “icon resimleri” ve “animated gif”leri kendi diskinize saklayın.
- Web üzerinde bir form doldurarak gönderdiğiniz bilgiler, eğer iletim modu güvenli (secure) değilse üçüncü kişiler tarafından görülebilir. Bu konuda dikkatli olmak gerekir.
- Önemli bilgileri, non-secure bir modda göndermeyin. Bazı tarayıcılar, bu gibi durumlarda kullanıcıyı uyarır. Kullandığınız Web listeleyicisi sizi uyarıyorsa, lütfen uyarıyı okuyun.

Web (WWW)'in Geleceđi

- 1994'ten sonra yaşananlar göstermektedir ki, bu konuda şimdiden tam bir tahmin yapmak imkansızdır.
- Web, deđişik konular ve disiplinler için bir sunu ortamıdır.
- Görsel zenginlik, kullanım kolaylığı ve süreklilik/akıcılık içeren pek çok öge Web ile bütünleşik bir yapıda olmaktadır ve yenileri de olacaktır.
- Mevcut duruma ve gelişmelere bakıldığında Web tabanlı sistemlerin önümüzdeki günlerde aşağıdaki alanlarda yoğun kullanılacağını söyleyebiliriz.
- **Yayıncılık, Basın-Yayın :**
 - Daha şimdiden, Web ortamları, basın-yayın kuruluşları ve yayınevleri tarafından çok etkin kullanılmaya başlanmıştır. Önümüzdeki yıllarda şu an şaşırarak ve merak içinde izlediğimiz bu çalışmalar rutin haline gelebilir ve kağıtsız bir yayıncılık ortamı Web üzerinde boy gösterebilir. Bunun ilk örnekleri, daha çok bilimsel dergilerde kendini göstermiştir. Her gün artan sayılardaki bilimsel dergileri on-line okuyabiliyoruz.
- **Bilgi Sistemleri ve Veri Bankaları:**
 - Deđişik konulardaki bilgileri içeren “Sanal Kütüphaneler”in daha hiyerarşik bir yapılanma içinde boy göstermeleri oldukça yakındır. Sanayi, tarım, eğitim, KOBİ'ler, BOBİ'ler, hükümet kaynakları vb gibi konularda ilk elden bilgilerin verildiđi merkezlerin sayıları her geçen gün artmaktadır. Ayrıca, araştırma kuruluşları ve üniversiteler, yaptıkları araştırmalar ile ilgili bilgileri daha sistematik ve Web ile daha bütünleşik bir yapıda sunmaktadırlar.

Web (WWW)'in Geleceđi

■ Web Üzerinden Oylama:

- Web, genel/yerel seçimler için olmasa da, daha küçük çaplı oylamalar için kullanılabilir. Neden olmasın? Kişiler, Web üzerinden bazı formlar doldurup bunları gerekli merkezlere gönderebilir. Demokrasilerin işleyişinde oylamaların amacı mümkün olduğunca çok insanın oylamaya katılmasıyla daha sağlıklı işlediğine göre, eldeki tüm imkanlar bu iş için kullanılabilir. Web de bunlardan biri.

■ Canlı ve Etkileşimli Eğlence Ortamları:

- Televizyon, insanların eğlence, haber alma/bilgilenme ihtiyaçlarını karşılamada çok önemli bir araçtır. Ancak, büyük oranda tek yönlü bir medya ortamı. Web üzerinde interaktif (etkileşimli) yayıncılık yapılabilmesi için herşey var. Web kullanıcıları, Web ortamında seyrettikleri şovlara bile katılabilirler.

■ Haber :

- Klasik haber medyası (gazete, dergi, tv, radyo), haberleri (diğer programlarında olduğu gibi) kendileri seçerek sunmakta. İstersek de istemezsek de bir haber saatında, ilgili yayıncının seçtiđi haberleri seyredeceğiz. Gazete için bu biraz daha esnek ama, orada da, hangi haberin daha önemli olduğuna yine bazı kişiler karar veriyor.

■ Uzaktan Eğitim:

- Üniversiteler ve diğer bazı kuruluşlar, yıllardır, fiziksel olarak uzak merkezlerde oturan kişiler, öğrenciler için “uzaktan eğitim” vermenin hazırlığını yapmaktadırlar. Fırat Üniversitesi’nde Sanal Üniversite için proje çalışmaları devam etmektedir. Gelişen ağ teknolojisi ve Web temelli ortamlar bu konuda ideal çözümler olarak karşımızdadırlar. Uzaktan eğitim, sadece öğrenciler, üniversiteler ile sınırlı değildir. Artık bir gereksinim halini alan “sürekli eğitim” mantığı içinde, değişik disiplinler için sürekli eğitim programlarının gerekliliđi günümüzde tartışılmaktadır.

■ Uzaktan Konferans:

- Bir konferansa oturduğumuz yerden katılıp, bildirimizi sunabiliriz. Yolculuk ve konferans masrafları ve geçen zamanı düşünürsek, konferanslarda Web üzerinden bildiri sunmak bundan sonraki yıllarda daha da uygunlaşacaktır.

Web (WWW)'in Geleceđi

- Gelecekte, kendi ilgili alanımıza giren konuları içeren haber ortamlarını Web üzerinde dizayn edebilecek gibiyiz.
- Söz gelimi, o gün dünyadaki tüm spor olaylarını ya da bilimsel toplantılar ile ilgili haberleri izlemek istediğimizde yapmamız gereken sadece bu alanları belirlemek ve “Haber İzleme Programımızı” bu kişisel haberler içeriğine yönlendirmek olmalı.
- Microsoft ve CNN gibi kuruluşlar, kişilerin isteklerine göre (on demand) haber formatlarını hazırlayan sistemler üzerinde çalışıyorlar.

Internet ve Bilgi Güvenliği

- Bilgi Güvenliği;
 - Bilişim ürünleri/cihazları ile bu cihazlarda işlenmekte olan verilerin bütünlüğü ve sürekliliğini korumayı amaçlayan çalışma alanıdır.
- Bilgi Güvenliğinin Amacı
 - Veri Bütünlüğünün Korunması
 - Erişim Denetimi
 - Mahremiyet ve Gizliliğin Korunması
 - Sistem Devamlılığının Sağlanması



Tehdit Türleri

Dahili Tehdit Unsurları

- Bilgisiz ve Bilinçsiz Kullanım
- Kötü Niyetli Hareketler

~ % 80

Harici Tehdit Unsurları

- Hedefe Yönelmiş Saldırıları
- Hedef Gözetmeyen Saldırıları

~ % 20

Dahili Tehdit Unsurları

■ Bilgisiz ve Bilinçsiz Kullanım

- Temizlik Görevlisinin Sunucunun Fişini Çekmesi
- Eğitilmemiş Çalışanın Veritabanını Silmesi



■ Kötü Niyetli Hareketler

- İşten Çıkarılan Çalışanın, Kuruma Ait Web Sitesini Değiştirmesi
- Bir Çalışanın, Ağda “Sniffer” Çalıştırarak E-postaları Okuması
- Bir Yöneticinin, Geliştirilen Ürünün Planını Rakip Kurumlara Satması

Harici Tehdit Unsurları

■ Hedefe Yönelmiş Saldırılar

- Bir Saldırganın Kurum Web Sitesini Değiştirmesi
- Bir Saldırganın Kurum Muhasebe Kayıtlarını Değiştirmesi
- Birçok Saldırganın Kurum Web Sunucusuna Hizmet Aksatma Saldırısı Yapması



■ Hedef Gözetmeyen Saldırılar

- Virüs Saldırıları (Melissa, CIH – Çernobil, Vote)
- Worm Saldırıları (Code Red, Nimda)
- Trojan Arka Kapıları (Netbus, Subseven, Black Orifice)



Saldırı Kavramı

- Kurum ve şahısların sahip oldukları tüm değer ve bilgilere izinsiz erişmek, zarar vermek, maddi/manevi kazanç sağlamak için bilişim sistemleri kullanılarak yapılan her türlü hareket dijital saldırı olarak tanımlanabilir.
- `Saldırgan` (hacker) sisteminizin güvenliğini geçmeyi ve kendi amaçları doğrultusunda kullanmayı amaçlayan kişidir.

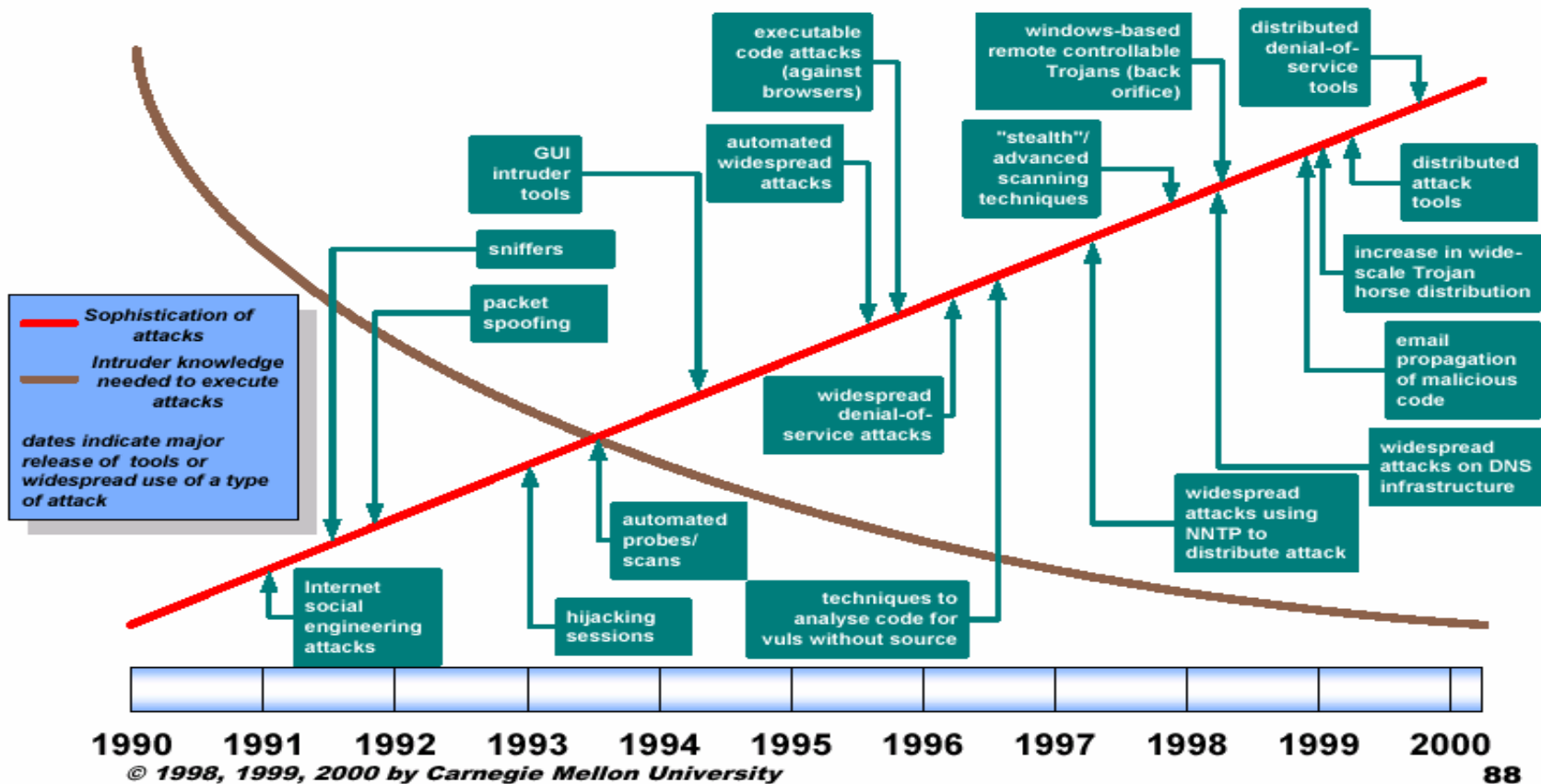
Saldırgan Türleri

- Profesyonel Suçlular
- Genç Kuşak Saldırganlar
- Kurum Çalışanları
- Endüstri ve Teknoloji Casusları
- Dış Ülke yönetimleri



Saldırı Kalitesi ve Saldırgan Yeteneklerinin Gelişimi (CERT/CC)

Attack Sophistication vs. Required Intruder Knowledge

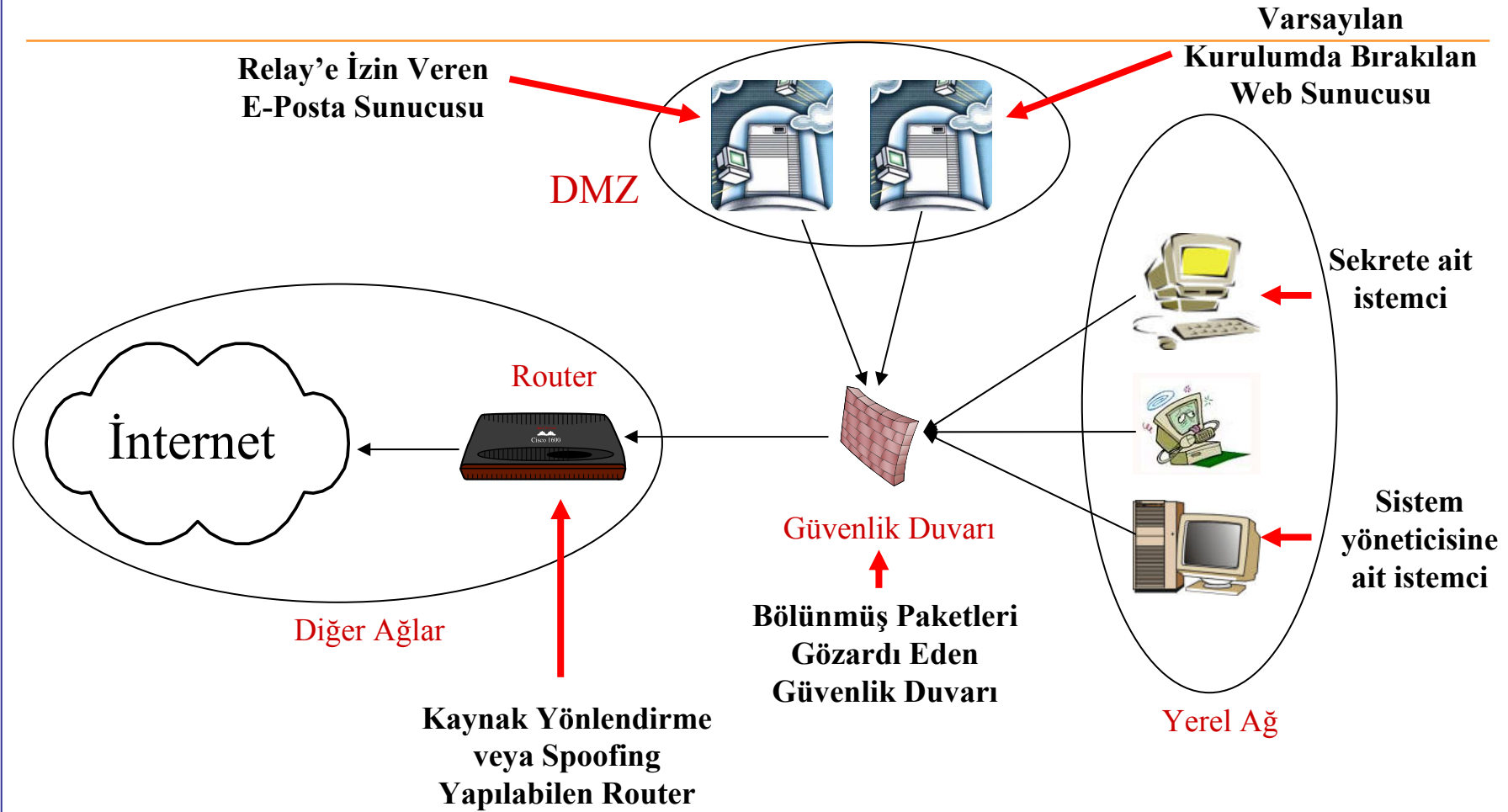


Saldırganın Amaçları

- Maddi Menfaatler
- Rekabet Avantajı
 - Politik
 - Ekonomik/Ticari
- Ek Kaynaklara Erişme İsteği
- Kişisel Öfke veya İntikam
- Merak veya Öğrenme İsteği
- Dikkatsiz Davranışlar



Ağda Bulunan ve Potansiyel Risk İçeren Sistemler



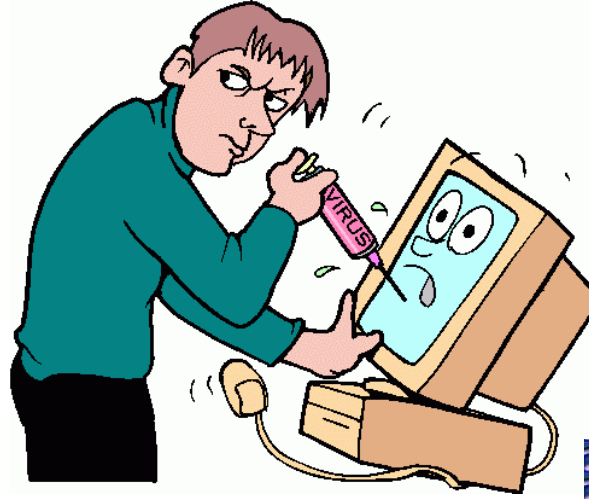
Saldırı Yöntemleri

- Hizmet Aksatma Saldırıları
- Dağıtık Hizmet Aksatma Saldırıları
- Ticari Bilgi ve Teknoloji Hırsızlıkları
- Web Sayfası İçeriği Değiştirme Saldırıları
- Kurum Üzerinden Farklı Bir Hedefe Saldırmak
- Virüs , Worm , Trojan Saldırıları
- İzinsiz Kaynak Kullanımı



Saldırılarda Sıkça Kullanılan Teknikler

- Sosyal Mühendislik
- Ağ Haritalama
- Uygulama Zayıflıkları
- Yerel Ağ Saldırıları
- Spoofing
- Hizmet Aksatma Saldırıları (Dos , DDos)
- Virüs, Worm , Trojan Kullanımı



Virüs, Worm ve Trojan Tehlikeleri

- Virüs, Worm ve Trojan'lar hedef gözetmeksizin bulaşan ve genelde sistemin işleyişini durdurmaya çalışan küçük yazılımlardır
- Virüs'ler e-posta, veri taşıma ortamları (disket, cd, dvd vb.) ve web sayfaları ile yayılabilir (Melisa, CIH)
- Worm'lar, Virüs'lerin kullandıkları yöntemlere ek olarak, uygulama/işletim sistemi zayıflıkları ile saldırılar düzenleyebilir ve bu şekilde de yayılabilir (Code Red, Nimda)
- Trojan'lar ancak ilgili uygulama çalıştırıldığında etkili olmaktadır (Netbus, Subseven)



Virüs, Worm ve Trojan'ları Önleme Yöntemleri

- **Anti-Virüs sistemleri, tüm istemci ve sunucuları koruyacak şekilde kullanılmalıdır**
- **Worm saldırılarını engelleyebilmek için Saldırı Tespit Sistemleri (eğer mümkün ise Güvenlik Duvarı) üzerinde önlemler alınmalıdır**
- **İnternet üzerinden kurumsal ağa gelen FTP, HTTP, SMTP, POP3, IMAP gibi protokollere ait paketler Anti-Virüs sistemleri tarafından incelenmeli, mümkün ise Anti-Virüs ağ geçidi kullanılmalıdır**

Saldırıya Uğrayabilecek Değerler

- Kurum İsmi, Güvenilirliği ve Markaları
- Kuruma Ait Özel / Mahrem / Gizli Bilgiler
- İşin Devamlılığını Sağlayan Bilgi ve Süreçler
- Üçüncü Şahıslar Tarafından Emanet Edilen Bilgiler
- Kuruma Ait Adli, Ticari Teknolojik Bilgiler

Görülebilecek Zararın Boyutu

- **Müşteri Mağduriyeti**
- **Kaynakların Tüketimi**
- **İş Yavaşlaması veya Durdurulması**
- **Kurumsal İmaj Kaybı**
- **3. Şahıslara Karşı Yapılacak Saldırı Mesuliyeti**



Güvenlik İhtiyacının Sınırları

- **Saldırıya Uğrayabilecek Değerlerin, Kurum İçin Arzettiği Önem Seviyesi Güvenlik İhtiyacının Sınırlarını Belirlemektedir.**

Genel Güvenlik Önlemleri

- **Bir Güvenlik Politikası Oluşturulmalı**
- **Tüm Ağ Sorun Kaldırabilecek Şekilde ve Politikada Belirlendiği Gibi Yapılandırılmalı**
- **Düzenli Olarak Yedekleme Yapılmalı ve Yedekler Kontrol Edilmeli**
- **Gerek Duyulan Güvenlik Uygulamaları Kullanılmalı**
 - **Güvenlik (Ateş) Duvarı - FireWall**
 - **Saldırı Tespit Sistemi (IDS)**
 - **Anti-Virüs Sistemi**
- **Ağ Düzenli Olarak Denetlenmeli ve İzlenmeli**
- **Çalışanlar Politikalar ve Uygulamalar Konusunda Eğitilmeli**

Ateş (Güvenlik) Duvarı (FireWall)

- Bir sistemin özel bölümlerini halka açık bölümlerinden ayıran, insanların kendilerine tanınan haklardan daha fazlasını almalarını engelleyen yapılardır.
- Ağlar arası erişimi, kural tabanlı olarak belirler.
- Yazılım veya donanım tabanlıdır.
- Mimarileri
 - Statik Paket Filtreleme
 - Dinamik Paket Filtreleme (Statefull inspection)
 - Uygulama Seviyesinde Koruma (proxy)
- Türölü formatta kayıt ve uyarı sunabilirler



Saldırı Tespit Sistemleri (IDS)

- Saldırı Tespiti Sistem'leri (Intrusion Detection Systems), bilgisayar sisteminize ve ağ kaynaklarınıza olan saldırıları tespit etmek, sistemi izleyip anormal olan durumları saptamak ve bunlara karşı gerekli önlemleri almayı amaçlayan güvenlik sistemleridir.
- Saldırı Tespit Sistemleri denetlediği veriler açısından iki ana gruba ayrılabilir.
 - Ağ Bazlı:
Ör: Packet Sniffer, Network Monitors
 - Sunucu (host) Tabanlı:
Ör: Network Monitor, Host Monitor



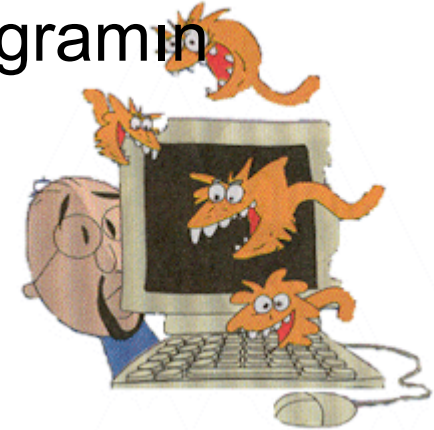
Saldırı Tespit Sistemleri (IDS)

Kullandığı teknikler açısından IDS iki ana gruptan oluşur:

- **Kalıp Eşleştirme (Signature) Sistemleri:** Önceden tespit edilmiş saldırıların eş zamanlı olarak işleyici tarafından karşılaştırılmasını esas alır.
Ör:\ Snort vb.
- **Anormallik Algılayıcı (Anomaly Detection) Sistemleri:** Sistemi önce öğrenen, istatistiksel olarak normal çalışma yapısını çıkaran sistemlerdir. Buna göre anormal davranışları yakalarlar.
Ör:\ Cylant Secure, NFR(Network Flight Recorder) vb.

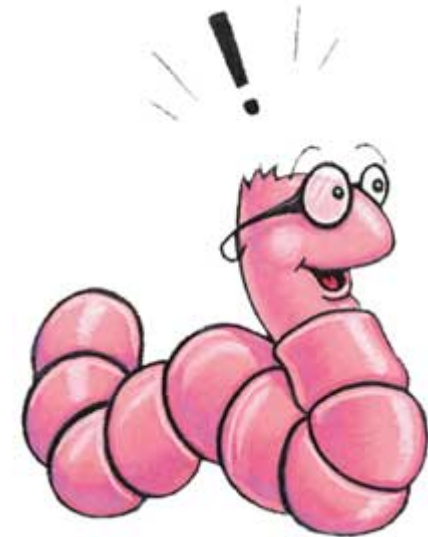
Virüsler

- RFC 1135'e göre virüs tanımı:
 - “Virüs”, işletim sistemleride dahil olmak üzere, kendini bir taşıyıcıya yerleştirerek yayılan bir kod parçasıdır.
 - Tek başına çalışamaz.
 - Aktif hale gelebilmesi için taşıyıcı programın çalıştırılması lazımdır.



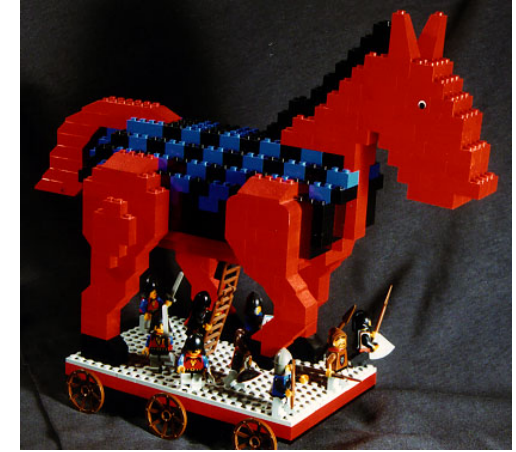
Kurtçuk (Worm)

- RFC 1135'e göre kurtçuk tanımı:
 - “Kurtçuk” taşıyıcısının kaynaklarını kullanarak tek başına çalışabilen ve çalışabilen tam bir kopyasını başka makineler üzerinde de oluşturabilen programlardır.



Truva Atları (Trojan Horse)

- Zararsız programcıklar gibi gözükürler
- Bulaştığı program normal seyrinde çalışır
- Yapacağı işleri arka planda çalışarak kullanıcıya hissettirmez
- Sistemde farkedilmeleri çok zor olabilir



Adware

- Kullanıcının, alışkanlıklarını izleyerek merkezi bir noktaya raporlayan, kullanıcıyı kendi üye sitelere yönlendirerek hit kazandırmak gibi korsan işlevler yaratan yazılım.



Virüsler sisteme nasıl girer?

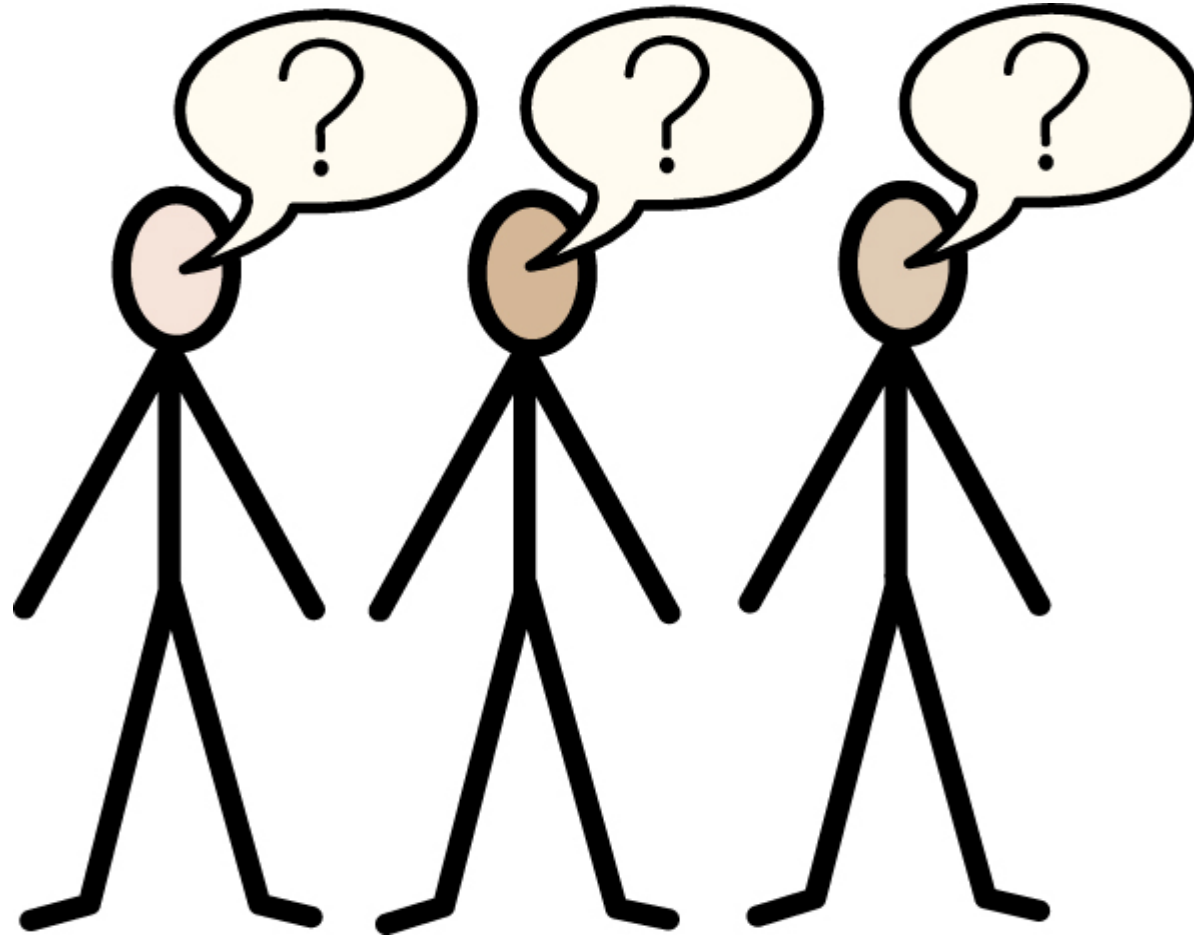
- Internetten çekilen programlar ile
- E-posta ekleri ile
- Ağdaki paylaşıma açık dosyalar ile
- Bilgisayarınıza taktığınız taşınabilir medya vasıtası ile



Virüslere karşı korunma

- Sisteme anti-virüs programı yüklenmeli
- Internetten çekilen dosyalar konusunda dikkatli olunmalı
- Bilinmeyen kaynaktan gelen e-posta'daki ekli dosyaları açılmamalı
- Paylaşılan taşınabilir medyalar virüs kontrolünden geçirilmeli
- Eğer bir programın virüslü olduğundan şüpheleniyorsanız o programı kullanmayın!
- Bir program satın aldığınızda üreticinin mühürünün yırtılmadığına emin olun

Soru - Cevap



TEŞEKKÜRLER

hasanbalik@gmail.com