

# KİŞİSEL BİLGİSAYARLAR ve İNTERNET GÜVENLİĞİ



**Öğr. Gör. Özgür ZEYDAN**  
Zonguldak Karaelmas Üniversitesi  
Enformatik Bölümü  
ozgurzeydan@yahoo.com

# GİRİŞ

- Gün geçtikçe internet erişimi olan kişisel bilgisayarların sayısı sürekli artmaktadır.
- Savunmasız bilgisayarların internet ortamında maruz kalacağı tehlikeler de artmaktadır.

Bu bildiride;

- tehlikelere karşı alınması gereken basit fakat etkili yöntemleri açıklanacaktır.
- Microsoft Windows XP'nin nasıl daha güvenli hale getirileceği anlatılacaktır.
- “Kişisel kullanım için ücretsiz” olan güvenlik yazılımlarından bazıları önerilecektir.

# İnternet Ortamındaki Olası Tehlikeler

- İşletim sistemi açıkları
- Kullanıcı hesapları açıkları
- Paylaşımlar ve hizmetler
- Web tarayıcılarının açıkları
- Güvensiz yazılımlar ve casus yazılımlar
- Ağ ve internet üzerinden gelebilecek tehlikeler: virüsler, solucanlar, truva atları ve hacker saldırıları
- Tuş kaydediciler ve olta yöntemleri
- Numara çeviriciler
- Diğer olası tehlikeler

# İşletim Sistemi Açıkları

- Her işletim sisteminde açık kodlar vardır.
- Üretici firma bu açıkları fark ettiğinde yama ve güncelleme dosyaları yayınlar.
- Microsoft Windows XP işletim sisteminin açıklarını kapatmak için <http://windowsupdate.microsoft.com>
- Hackerlar en son yama ve güncellemeleri takip eder, bu nedenle “**Otomatik Güncellemeler**” mutlaka etkin olmalıdır.

# İşletim Sistemi Açıkları

MS Windows XP

➤ *Denetim Masası*

=> *Sistem  
Özellikleri =>*

*Otomatik  
Güncelleştirmeler*

The screenshot shows the 'Sistem Özellikleri' (System Properties) dialog box in Windows XP, with the 'Otomatik Güncelleştirmeler' (Automatic Updates) tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar are four tabs: 'Genel', 'Bilgisayar Adı', 'Donanım', and 'Gelişmiş'. The 'Otomatik Güncelleştirmeler' tab is active, showing a blue header with a shield icon and the text 'Bilgisayarınızı korumaya yardımcı olun'. Below this, there is a paragraph of text explaining that Windows can check for and install updates automatically. A link 'Otomatik güncelleştirmeler nasıl çalışır?' is provided. At the bottom, there are three radio buttons for update settings: 'Her zaman otomatik olarak güncelleştir' (selected), 'Her zaman güncelleştirme teklifleri için bildirimler gönder' (disabled), and 'Güncelleştirmeleri manuel olarak yükleyin' (disabled). The selected option is highlighted with a red box. Below the radio buttons, there is a green shield icon with a checkmark and the text 'Otomatik olarak önerilen güncelleştirmeleri karşıdan yükle ve kur:'. At the bottom, there are two dropdown menus: 'Her gün' and 'saat: 03:00'.

- Gereksiz bütün kullanıcı hesapları risk faktörüdür.

Microsoft Windows XP

- *Denetim Masası => Kullanıcı Hesapları*

- Sınırlı yetkilere sahip olan bir kullanıcı hesabı oluşturmak ve İnternet kullanırken bu hesap ile oturum açmak bizi internet üzerindeki olası tehlikelere karşı korur.

- Daha riskli durumlarda *sahte administrator* hesabı kullanarak hedef şaşırtılabilir.

# Sahte Administrator Hesabı İle Hedef Şaşırtma

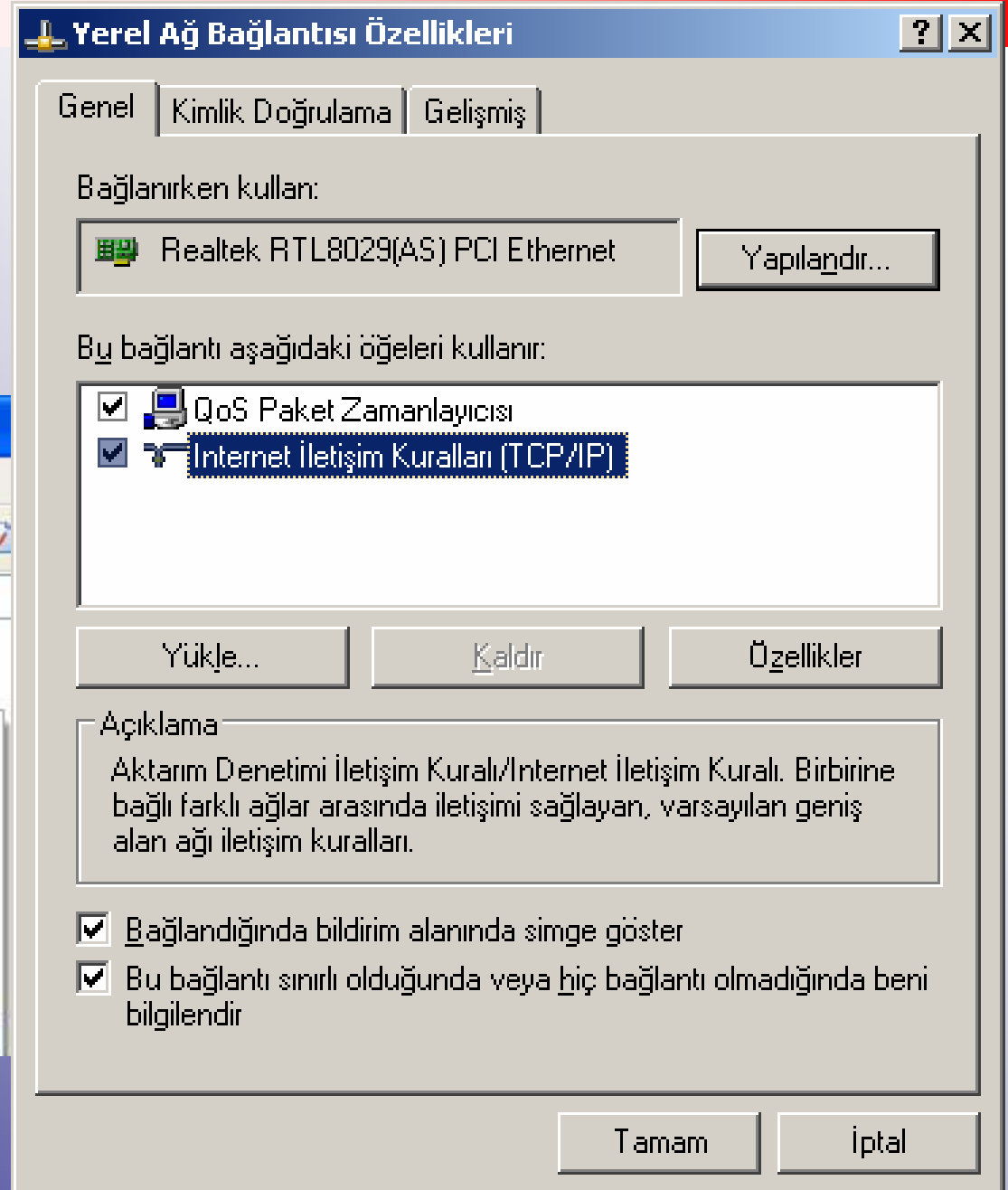
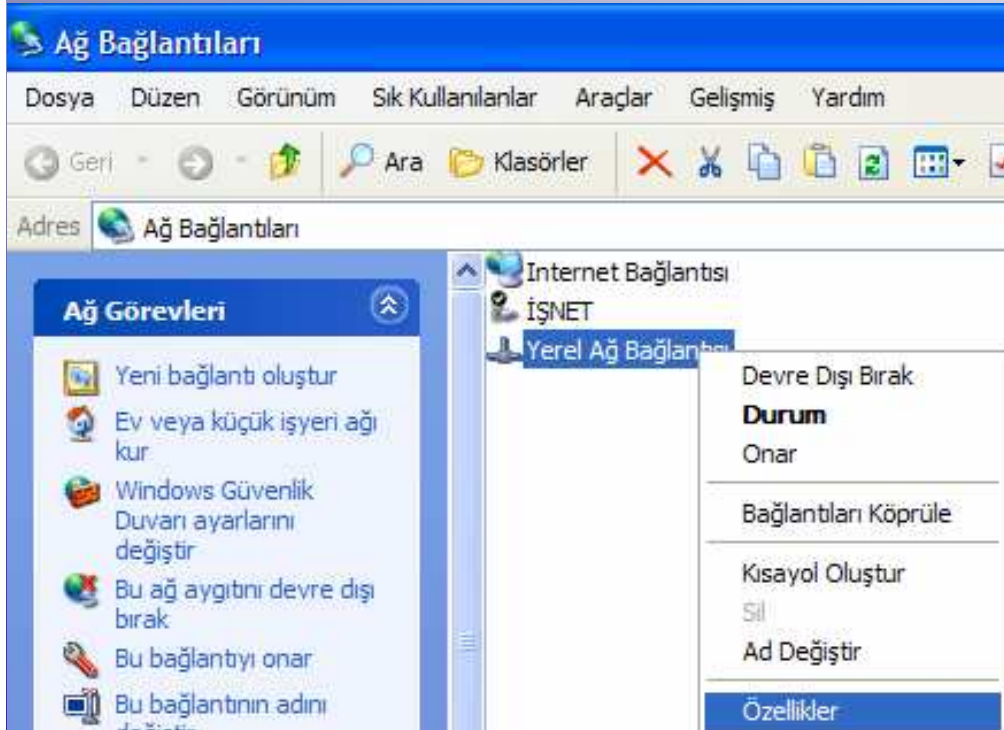
Hesap Adı	Hesap Türü	Açıklama
Administartor	Sınırlı kullanıcı	Sahte yönetici hesabı, güçlü bir şifre ile korunmuş yanlış hedef. Şifresi kırılrsa bile bilgisayarımızın önemli ayarları değiştirilemez
user1	Sınırlı kullanıcı	Günlük kullanım ve internet kullanımı için
user2	Sistem yöneticisi	Gerçek sistem yöneticisi hesabı

# MS Windows XP'de Gereksiz Paylaşımlar ve Protokoller

- Bilgisayarımız bir bilgisayar ağının parçası değilse veya dosya ve yazıcı paylaşım gibi servisler kullanılmıyorsa bu servisler mutlaka kapalı tutulmalıdır.
- Sadece internete bağlanmak için ihtiyaç duyduğumuz protokol **TCP/IP** protokolüdür.
- QoS Paket Zamanlayıcısı protokolü arka planda sistem güncellemeleri için gerekli, herhangi bir tehlikesi yok.

# Ağ Bağlantısı Özellikleri

- Denetim Masası => Ağ Bağlantıları => Yerel Ağ Bağlantısı özellikleri



# MS Windows XP'de Gereksiz Hizmetler

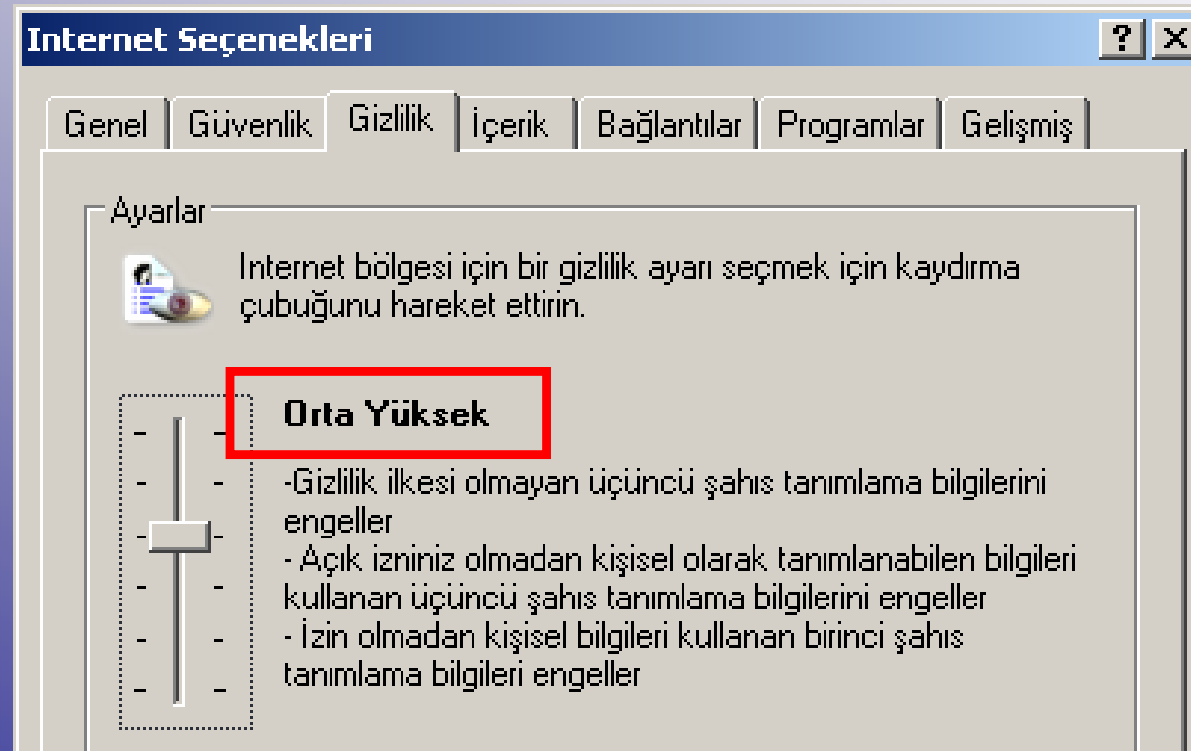
- *Denetim Masası => Yönetimsel Araçlar => Hizmetler*
- Kişisel bilgisayarlarda kullanılmıyorsa devre dışı olması gereken hizmetler:

<b>Hizmetin Adı</b>	<b>Açıklamalar</b>
Messenger	Bu hizmet kapatılarak sistemimizi spam e-postalara ve reklamlara karşı koruyabiliriz.
Uzaktan Kayıt Defteri	Başka bir kullanıcının ağ üzerinden kayıt defterini değiştirmesini sağlar, kullanılmıyorsa devre dışı olmalıdır
Netmeeting Remote Desktop Sharing	Başka bir bilgisayarı ağ üzerinden yönetmeye yarayan bu hizmet kullanılmıyorsa devre dışı olmalıdır.

- MS İnternet Explorer ile Outlook Express (e-posta istemcisi) hackerların hedefidir.
- MS İnternet Explorer ve Outlook Express için yama ve güncellemeler  
<http://windowsupdate.microsoft.com>
- MS İnternet Explorer'ı zararlı web sitelerine karşı korumak için ücretsiz olan *SpywareBlaster* adlı yazılımı <http://www.javacoolsoftware.com> web sitesinden indirip kullanmak mümkündür.

# MS İnternet Explorer ile daha güvenli sörf

- Araçlar => İnternet Seçenekleri...
- Gizlilik ayarı en az “Orta Yüksek” seviyesinde olmalıdır.



## ➤ Web Tarayıcıları:

- ❖ **Mozilla Firefox** (<http://www.mozilla.com/en-US/firefox/>)
- ❖ **Opera** (<http://www.opera.com>)

## ➤ e-posta istemcileri

- ❖ **Mozilla Thunderbird** (<http://www.mozilla.com/en-US/thunderbird/>)

# Güvensiz Yazılımlar ve Casus Yazılımlar

- **Güvensiz yazılımlar** illegal olarak kopyalanmış veya internetteki korsan sitelerden indirilmiş yazılımlar olup içlerinde bilgisayarımıza zarar verebilecek virüs, truva atı, tuş kaydedici ve her türlü casus yazılımı içlerinde barındırabilirler.
- **Casus yazılımlar** ise internette gezdiğimiz web sitelerinin kayıtlarını tutup bizden habersiz başkalarına gönderen, karşımıza istemediğimiz reklam pencerelerinin gelmesini sağlayan, bilgisayarımızdaki şahsi dosyalarımızı başkalarına gönderebilen, bilgisayarımızın performansını düşüren ve internet erişimini gereksiz yere meşgul eden istenmeyen yazılımlardır.



# Casus Yazılımlardan Korunmak

- Korsan yazılım kullanmaktan kaçınmak, lisanslı yazılım kullanmak
- Korsan web sitelerinden yazılım indirmemek
- Güvenli web sitelerinden yazılım indirmek. Bu sitelerde mutlaka “**No adware, no-spyware**” gibi uyarılar mevcuttur.
- Sırf bedava olduğu için ne olduğunu bilmediğimiz yazılımları bilgisayara yüklememek.
- Yazılım yüklerken “son kullanıcı lisans sözleşmesi”ne göz atmak. “**Ad-supported**” olarak desteklenen yazılımları bilgisayarımıza yüklememek.
- “Son kullanıcı lisans sözleşmesi”ni incelemek için **EULAlyzer** kullanılabilir  
(<http://www.javacoolsoftware.com/eulalyzer.html>)

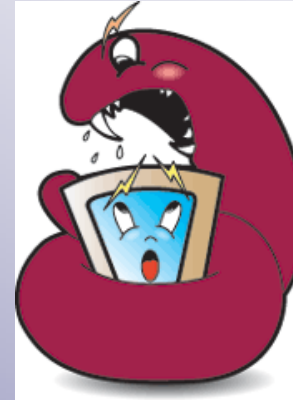
# Bilgisayarımızdaki Casus Yazılımları Temizlemek

Anticasus yazılımların içinde ücretsiz olanları:

- *Windows Defender* (<http://www.microsoft.com/athome/security/spyware/software/default.mspix>)
- *Ad-Aware* (<http://www.lavasoft.com>)
- *Spybot Search & Destroy* (<http://www.safer-networking.org/tr/index.html>)

# Ağ ve İnternet Üzerinden Gelebilecek Tehlikeler

- Ağ veya internet üzerindeki korunmasız bilgisayara **virüsler**, **truva atları**, **solucanlar**, **tuş kaydediciler** ve **casus yazılımlar** bulaşabileceği gibi kişisel verilerimize erişmek isteyen hackerlar da saldırıda bulunabilir.



- Bütün bu tehlikelerden korunabilmek için bilgisayarımızda hem **antivirüs** yazılımı hem de **güvenlik duvarı** yazılımı bulunmalıdır.

# Ücretsiz Antivirüs Yazılımları

Microsoft Windows XP için

➤ AVG Antivirus Free

❖ (<http://free.grisoft.com>)

➤ Antivir Antivirus

❖ (<http://www.avira.com>)

➤ Avast Home Edition

❖ (<http://www.avast.com>)

➤ Comodo Antivirus

❖ (<http://www.antivirus.comodo.com>)



# Ücretsiz Güvenlik Duvarı Yazılımları

- ZoneAlarm
  - ❖ (<http://www.zonelabs.com>)
- Sunbelt Kerio Personal Firewall
  - ❖ (<http://www.sunbelt-software.com/kerio.cfm>)
- Comodo Firewall
  - ❖ (<http://www.comodogroup.com>)
- NetVeda Safety.Net
  - ❖ (<http://www.netveda.com/consumer/safetynet.htm>)
- SoftPerfect Personal Firewall
  - ❖ (<http://www.softperfect.com/products/firewall>)
- Ashampoo FireWall FREE
  - ❖ (<http://www.ashampoo.com>)



# MS Windows XP Güvenlik Duvarı

- Microsoft Windows XP işletim sistemine servis paketi 2 ile dahil edilen güvenlik duvarı sadece **tek yönlü** çalışır. Bu güvenlik duvarı sadece internet üzerinden bilgisayarımıza gelen tehlikelerden bizi korur fakat bilgisayarımızdaki interneti kullanmak isteyen zararlı yazılımları engelleyemez.
- Microsoft'un 2007 yılında piyasaya süreceği Microsoft Vista işletim sisteminde de güvenlik duvarı bu şekilde çalışmaktadır.

# Tuş Kaydediciler ve Olta Yöntemleri

- Tuş kaydediciler genellikle **kredi kartı numara ve şifrelerini, internet bankacılığı hesap şifrelerini vb. önemli bilgileri çalmayı amaçlayan**, kullanıcıdan gizli olarak arka planda çalışan ve klavye üzerinden basılan her tuş ile farenin hareketlerini anlık olarak kaydeden zararlı yazılımlardır.

- korunmak için mutlaka:

- ❖ antivirüs + güvenlik duvarı

- ❖ ikisinin de aktif korumaları etkin olmalıdır.



# Olta Yöntemleri

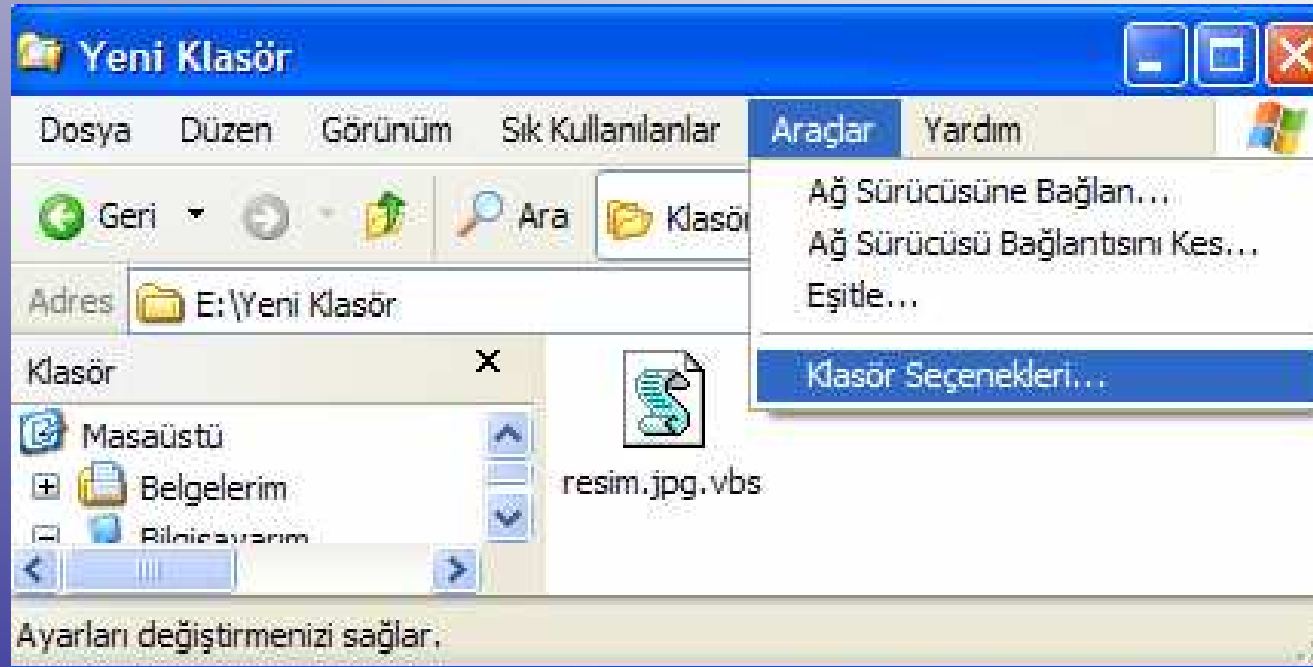
- Olta yöntemleri ise **internet bankacılığı şifresi, e-posta şifresi gibi bilgileri çalmak için** oturum açma sayfalarının sahtelerini yapmak ve kullanıcıyı bu sahte sayfaya yönlendirip şifrelerini çalmak için kullanılan yöntemlerdir.
- Korunmak için “hosts” dosyasının (**C:\WINDOWS\system32\drivers\etc\hosts**) bilginiz olmadan değiştirilmesini önlemektir.
- Anti casus yazılımlar:
  - ❖ **Windows Defender**  
(<http://www.microsoft.com/athome/security/spyware/software/default.msp>) sistemimizde yüklü ve aktif koruması etkin halde ise bu dosyada yapılacak olan her türlü değişikliğe karşı kullanıcıyı uyaracaktır.
  - ❖ Ayrıca **Spyware Blaster** adlı yazılım da hosts dosyasını şifreleyerek korumaktadır.

# Numara Çeviriciler

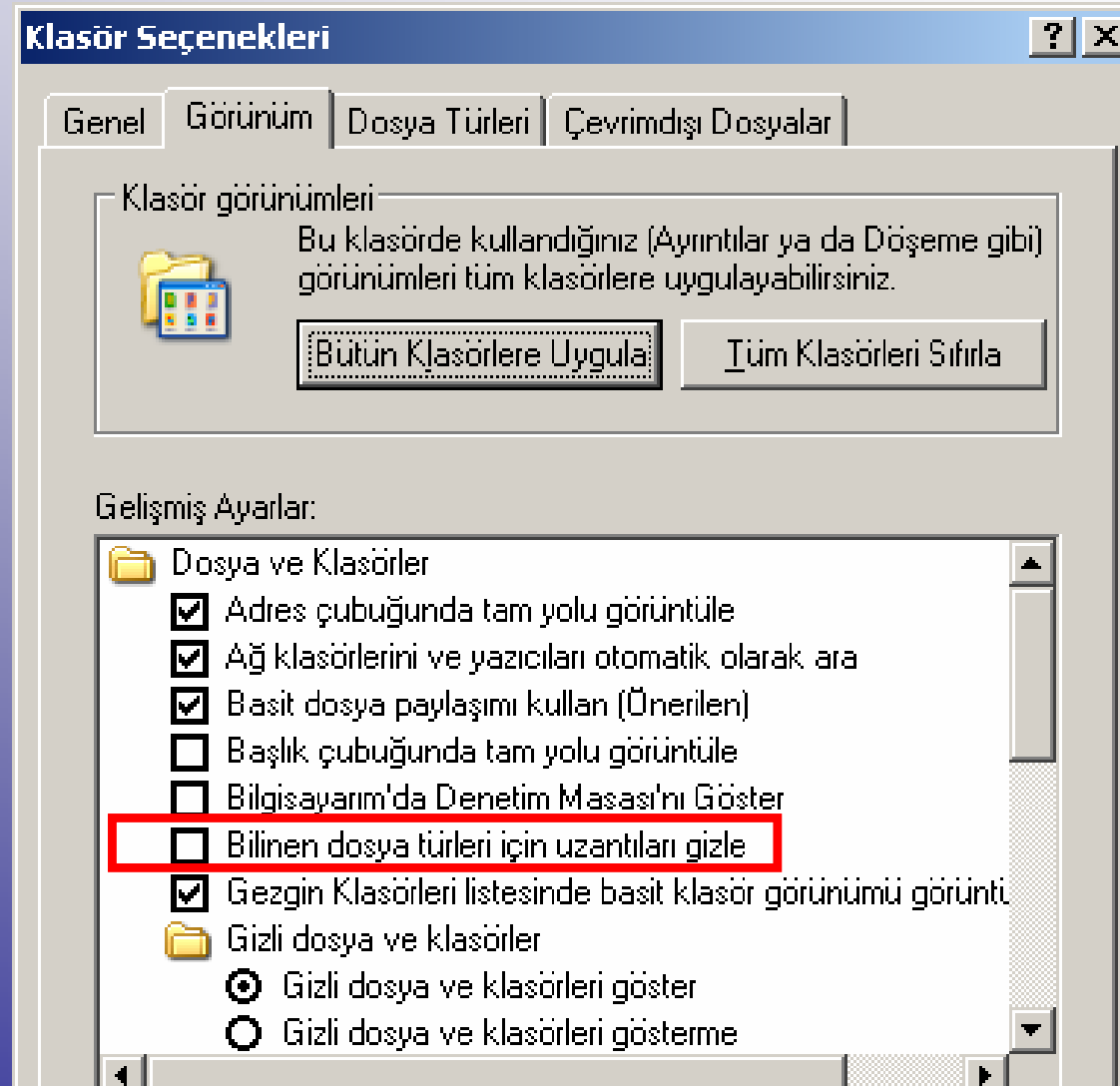
- İnternete “**çevirmeli bağlantı**” ile bağlanan kullanıcıların internet bağlantısını keserek milletler arası telefon numarası çevirir ve bilgisayarı internete yeniden bağlar.
- Herhangi bir web sitesinde “**sitemizdeki mp3leri bilgisayarınıza yüklemek için bu programı çalıştırın**” veya “**şifreli sayfalara erişebilmek için bu programı çalıştırın**” şeklinde bir yazı gördüğünüzde bunun numara çevirici olduğu kesindir.
- Bazı anti casus yazılımlar numara çeviricilere karşı da koruma sağlamaktadır.
- Ayrıca çevirmeli bağlantı ile internete erişilen telefon hattının milletler arası telefon görüşmelerine kapatılması çözüm olabilir.

# Diğer Olası Tehlikeler

- MS Windows XP işletim sisteminde klasör seçeneklerindeki “**Bilinen dosya türleri için uzantıları gizle**” seçeneği zararlı bazı kodların gizlenmesine yardımcı olabilir.



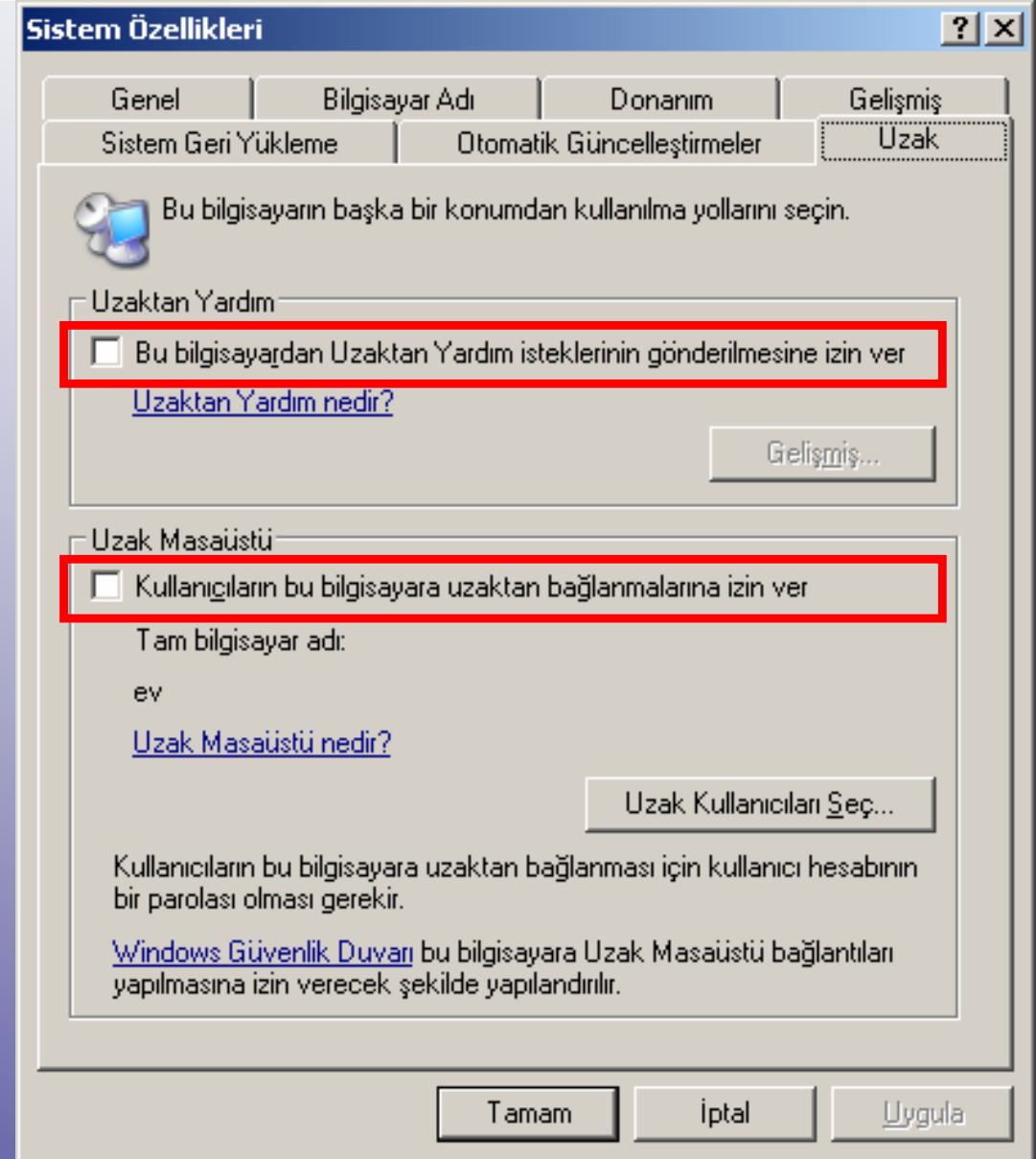
# “Bilinen dosya türleri için uzantıları gizle” seçeneğini devre dışı bırakmak



- Bu tip kablosuz modemlerde **eğer şifreleme uygulanmazsa** modem in etki alanı içindeki yabancı bir kablosuz ağ özelliği olan bilgisayar ağımıza erişebilmekte, internet bağlantımızı kullanabilmekte ve hatta özel verilerimize erişebilme imkanına sahip olmaktadır.
- Kotanın dolması ve fazla ücret ödeme durumu söz konusudur.
- Size ait internet bağlantısı kullanılarak sanal suçlar işlenebilir.
- **Kablosuz modemlerde mutlaka şifreleme işlemi kullanılmalıdır.**

# Uzaktan Yardım ve Uzak Masaüstü

- MS Windows XP
- *Denetim Masası => Sistem => Uzak*
- Kullanılmıyorsa mutlaka kapatılmalı



# Sonuç

- Savunmasız bir kişisel bilgisayar internete bağlandığı andan itibaren birçok tehlike ile karşı karşıyadır.

## Bilgisayarımızı ve interneti güvenli olarak kullanabilmek için:

- Antivirüs + Güvenlik Duvarı + Anticasus
- Ayrıca güvenlik yazılımlarını, işletim sistemimizi ve web tarayıcısı ile e-posta istemcisi gibi internet yazılımlarının en güncel hallerini kullanmak
- İnternet kullanırken de zararlı sitelere girilmemeli, güvenilir olamayan yazılımlar bilgisayara yüklenilmemeli ve çalıştırılmamalıdır.
- İşletim sistemimizin açıkları kapatılmalıdır.
- Bütün bu önlemler alındıktan sonra %99 güvenli olarak internet kullanabilirsiniz.

- Güvenli internet kullanımı dileğiyle...
- Dinlediğiniz için teşekkürler...
- Sorular???