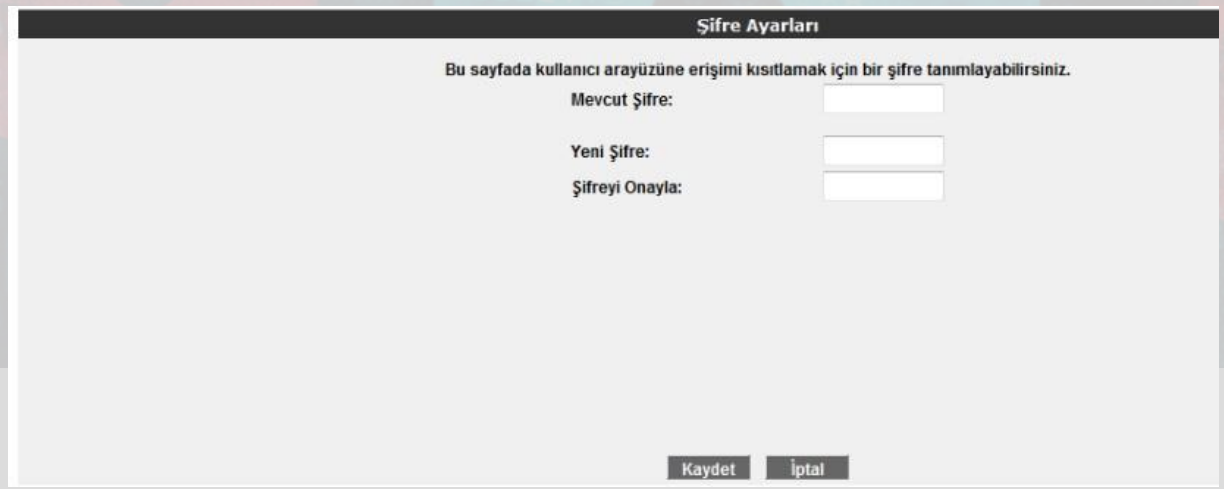
ECZANELERDE AĞ VE BİLGİSAYAR GÜVENLİĞİ

AĞ GÜVENLİĞİ NASIL SAĞLANIR ?

- Siber dünyaya giriş kapısı olarak modemlerimizi kullanmaktayız. Bilgisayarlarımız, cep telefonlarımız ve iot cihazlarımız, modemler üzerinden siber dünyadaki servislere ulaşarak, gerekli hizmetleri servislerden almaktadırlar. Modemler, dış ağlara açılan kapımız olduğu gibi kendi yerel ağımıza ulaşmak için de giriş kapısıdırlar.

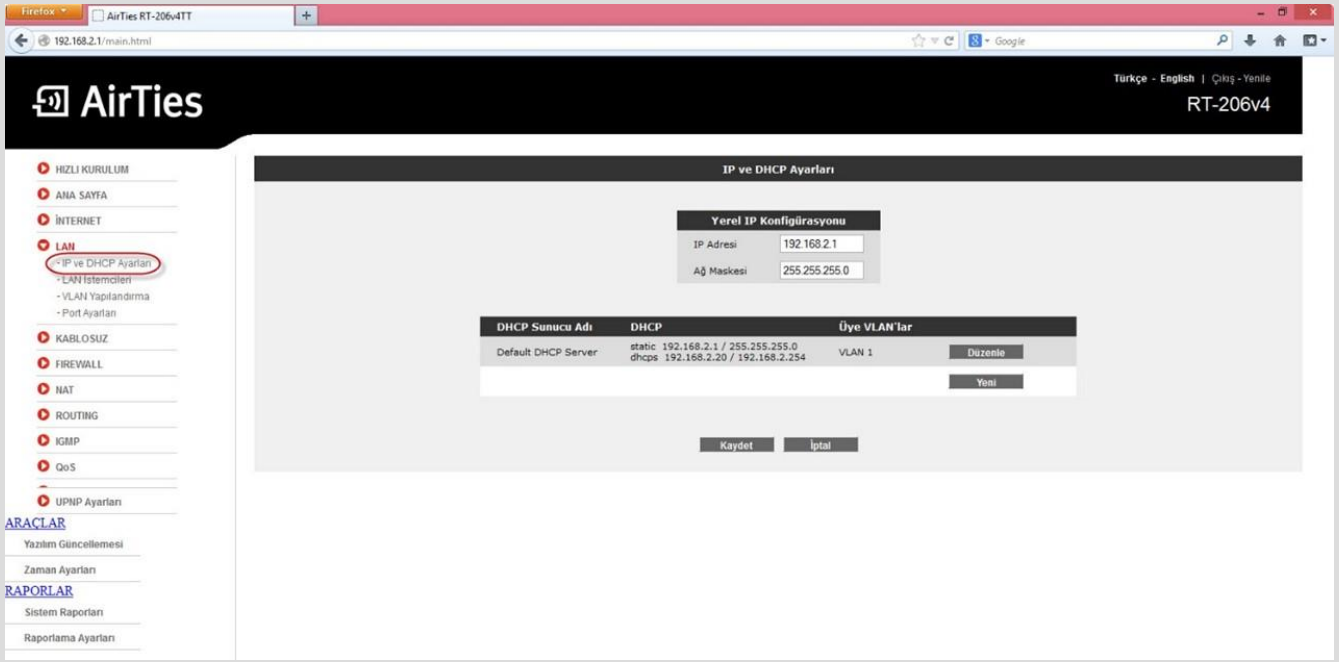
- Modemler marka ve modellerine göre farklı yazılım ve donanım yapıların da olmaktadırlar. Genel olarak modemlerin web ara yüzleri kullanılarak, kullanıcı adı ve şifre bilgileri ile yönetimleri sağlanmaktadır. Genelde kullanılan şifre ve kullanıcı adları: root ,admin ,ttnet ,1234 , password vb. dir. Bu gibi şifreleri olduğu gibi değiştirmeden bırakmak , kilidi olmayan ev gibi dışarıdan gelebilecek izinsiz girişlere sebep oluşturabilecektir.

- Modeminizin şifresini değiştirerek modeminizin güvenliğini arttırabilirsiniz. ***(bakınız: resim-1)***

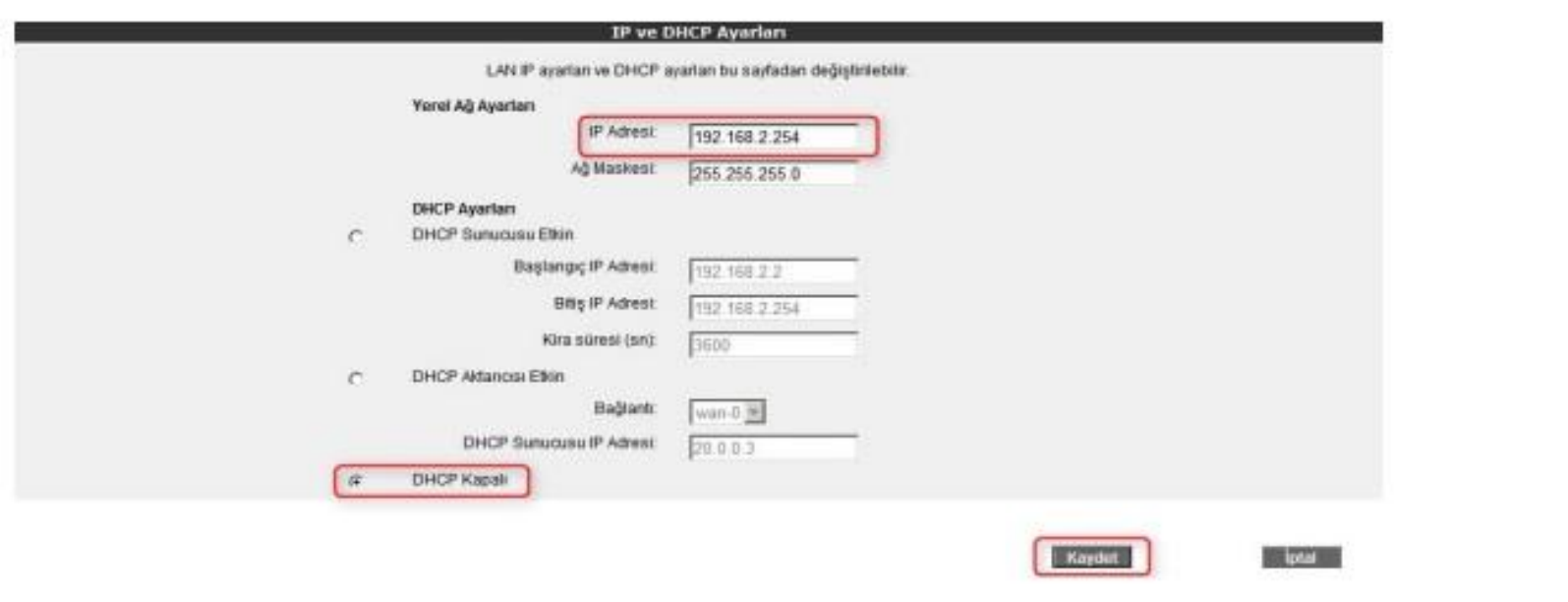


- Bunun için güvenli şifre kullanılmalıdır. Güvenli şifre en az 8 karakterden oluşmak kaydıyla şifrenizde büyük harf, küçük harf, rakam ve özel karakter (* ! . , @ gibi) bulunmalıdır. Güvenli şifre; tarih, şehir ,isim içermemelidir birbirinden farklı anlamsız karakter topluluğundan oluşmalıdır. Güvenli şifre vermenin amacı modeminize gelecek şifre deneme , bulma saldırılarını (Brute Force) şifrenin bulunabilirlik ihtimalini neredeyse imkansız kılacaktır.

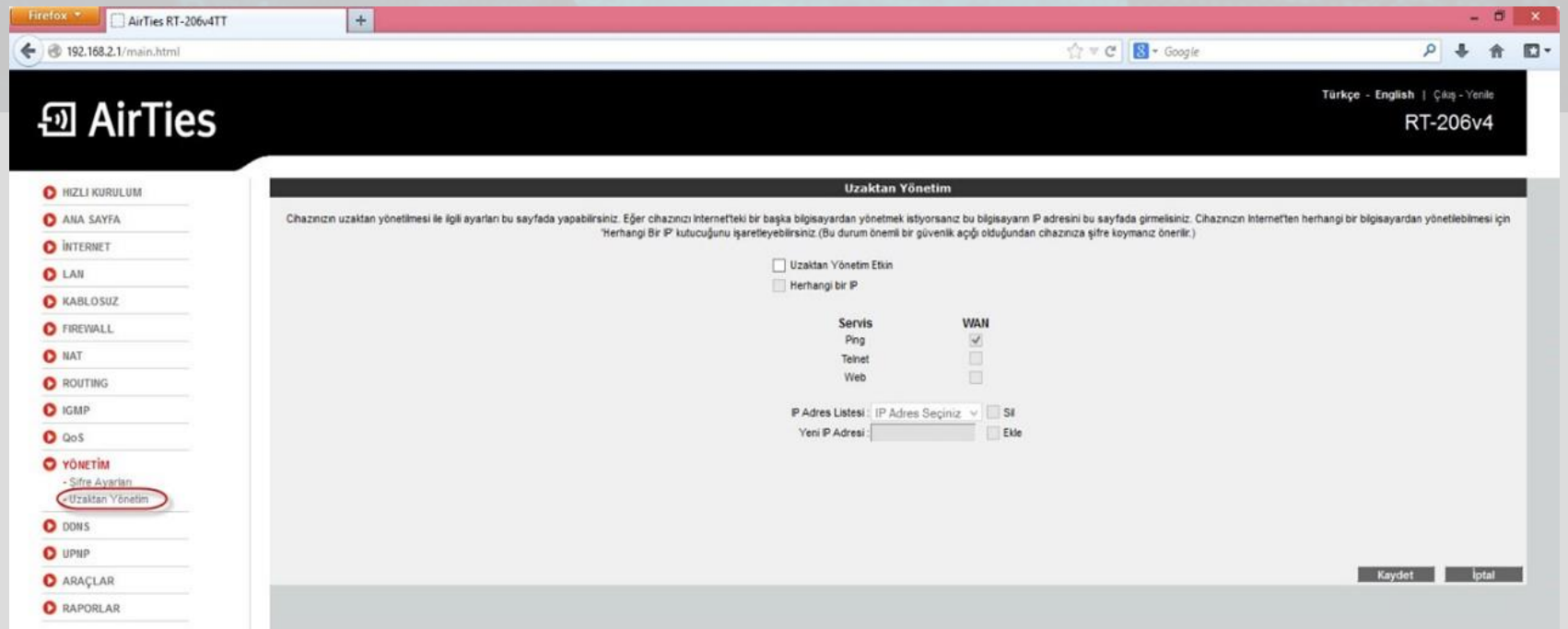
- Modem üzerinde, varsayılan yerel ağ IP yapılandırmasını değiştirmek gereklidir. Genelde modemlerde IP olarak 192.168.1.1, 192.168.2.1, 10.0.0.1 vb. Ip'ler kullanılmaktadır.
- Modeminiz içerisindeki varsayılan IP adresini değiştirerek , ağınızın IP adresinin tahmin edilememesini sağlamanız mümkün olacaktır. Örnek olarak 192.168.200.1, 10.10.1.1, 192.168.50.1 gibi ipler ile değiştirilerek, ağınızın bulunabilirliği azalacaktır.***(bakınız: resim-2)***



- ADSL modemlerinizde otomatik ip dağıtma servisi (DHCP) kapalı olmalıdır. Ağınıza izinsiz girişler bu şekilde minimize edilecektir. ***(bakınız: resim-3)***

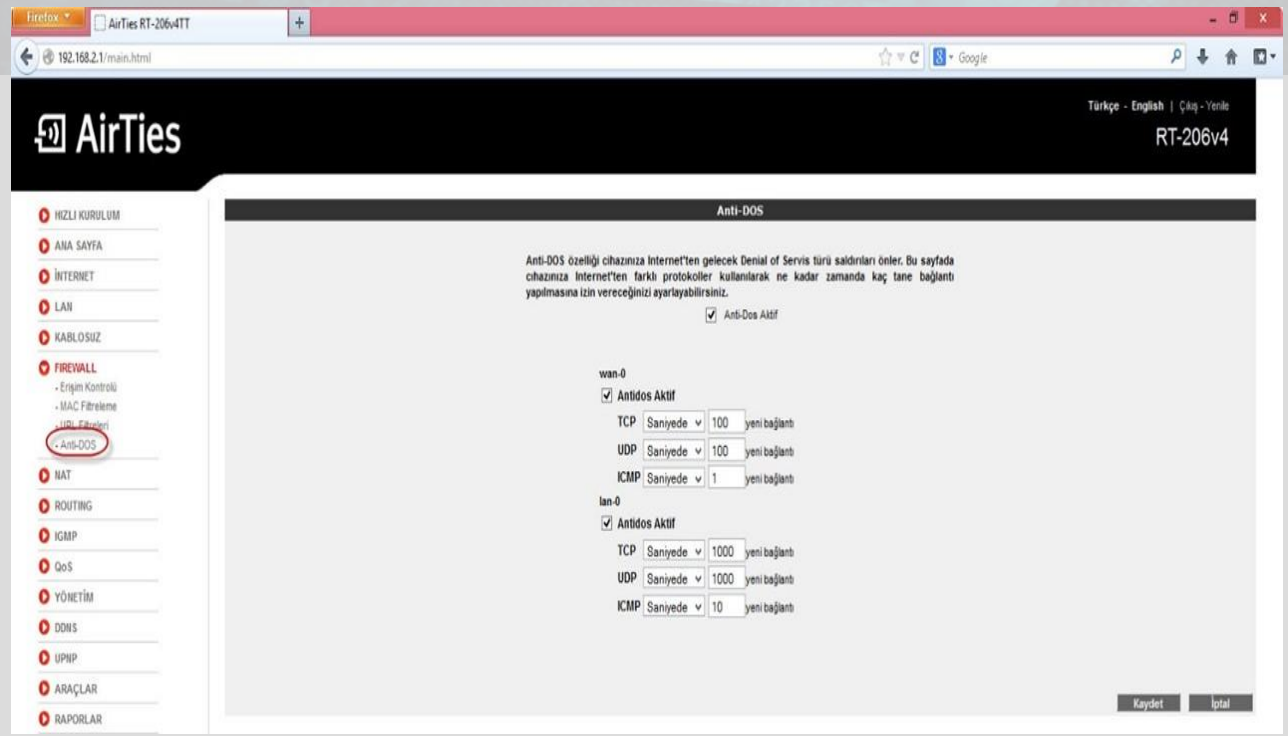


- Modeminize internet üzerinden erişim yapılamaması gereklidir. Bunun için modemin yönetim sayfasını sadece yerel ağa tanımlayarak erişimleri kısıtlayabilirsiniz yada modeminizin güvenlik duvarı üzerinden http , telnet , snmp gibi hizmetleri internete kapatarak güvenliği sağlayabilirsiniz. **(bakınız: resim-4)**



- Modeminiz de MAC adres filtrelemeyi aktif duruma getirebilirsiniz. Bu şekilde ağınıza kendi tanımladığınız MAC adresleri yani bilgisayarlar ve diğer cihazlar haricinde, bağlanmayı engelleyebilirsiniz. Bu gibi uygulamalar dışarıdan, ağınıza gelebilecek saldırılara karşı önlem oluşturacaktır.***(bakınız: resim-5)***

- Bazı modemlerde, anti-dos yani ddos atak engellemek için gerekli güvenlik uygulaması mevcuttur. Bu özelliğe sahip modeminiz var ise belirli bir zaman içerisinde, belirli protokollerden kaç tane istek alacağınızı belirterek, belirlenen istek üzerinde bir istek cihazınıza gelirse modeminiz bu özellik sayesinde gelen isteklere karşı ağınızı savunmaya geçecektir. ***(bakınız: resim-6)***



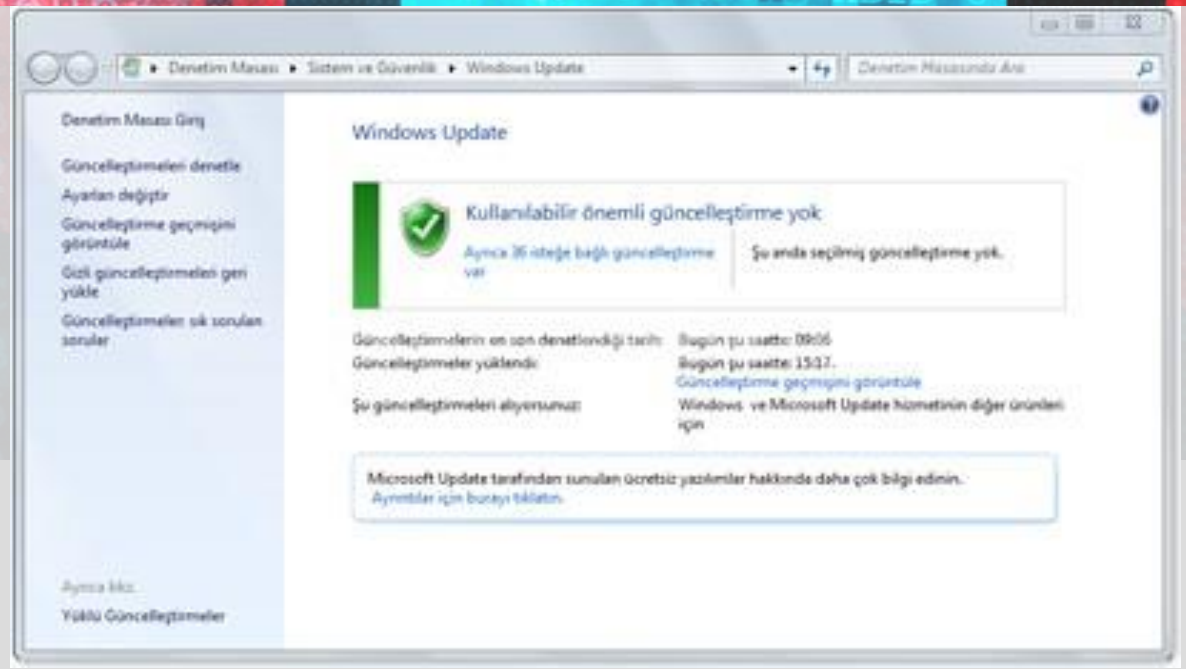

BİLGİSAYAR SİSTEMLERİNİN KORUNMASI ?

İŞLETİM SİSTEMİ:

- Bilgisayarlar çalışabilmesi için işletim sistemine ihtiyaç duyarlar. İşletim sistemleri bilgisayarlarda yaptığımız çalışmaları, internet kullanımını ve birçok uygulamayı gerçekleştirdiğimiz platformlardır.

- İşletim sistemleri güncel olmalıdır. Güvenlik için güncellemeler işletim sistemlerinin en önemli etkenlerinden biridir. İşletim sistemine yönelik güncellemelerin çoğu güvenliğe yönelik olmaktadır.

- Bu gibi güncellemeler işletim sisteminizde bulunan açıkları kapatarak işletim sistemi içerisindeki güvenliği artırmaya yardımcı olur.***(bakınız: resim-7)***



- Lisanssız (illegal)kullanılan işletim sistemi, gerekli güncellemeleri alamayacaktır. Bu sebeple internet üzerinden gelebilecek saldırılara açık olacaktır. Bununla birlikte lisanssız (illegal) kullanılan işletim sistemlerinde illegal kullanıma açan ve dağıtıma sunanlar tarafından içerisinde sizin bilmediğiniz ancak bu yapıyı hazırlayanlar tarafından, verilerinizi ele geçirebilecek , zararlı kod parçacıkları yerleştirilerek dağıtıma sunulmaktır. Dolayısı ile siz farkında olmadan bilgisayarınız saldırganlar tarafından kullanılıyor olabilir!!!

ANTİVİRUS PROGRAMLARI:

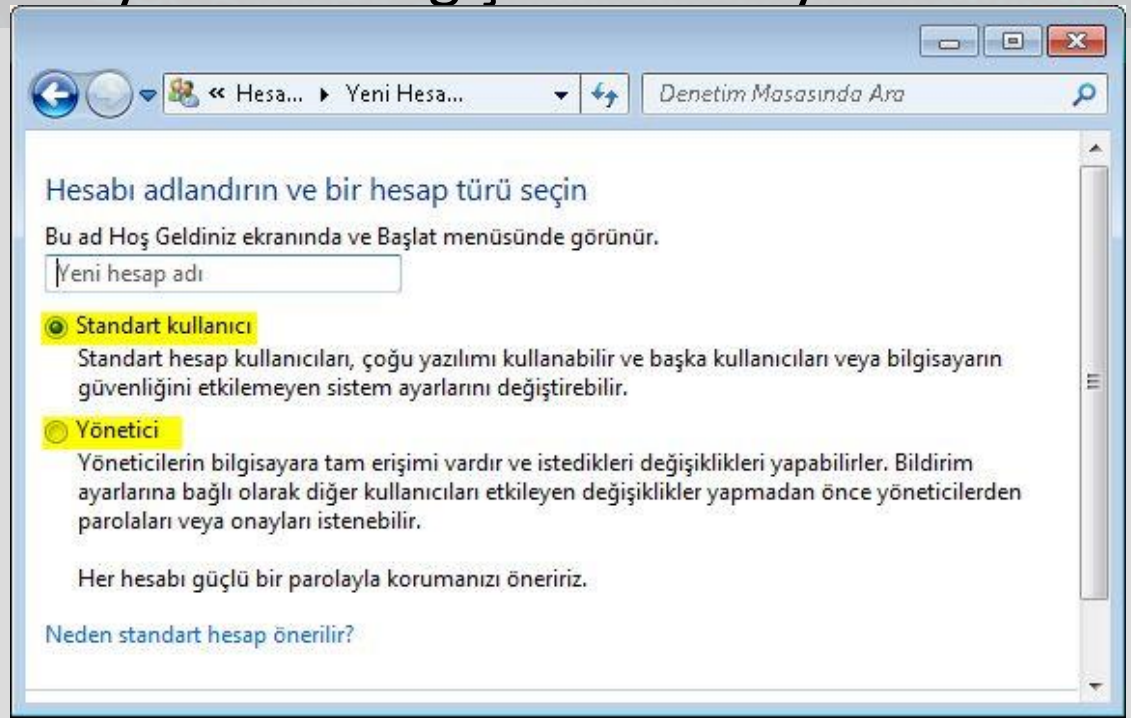
- İnternette ciddi sayıda casus yazılımlar, keyloggerlar ve malware vb. bir çok çeşitte zararlı programlar bulunmaktadır.

- Anti virüs yazılımınızı sürekli güncel tutmak zorundayız. Çünkü internette, bilgisayarınıza zarar verecek yazılımlar sürekli kendini güncellemekte ve yenilemektedir. Anti virüs yazılımlarınızı güncel tutarak, zararlı yazılımlara karşı bilgisayarlarınızı korumuş olursunuz.

- Belirli periyotlarda anti virüs yazılımları ile bilgisayarınızı taratmalıyız ve anti virüs yazılımınızı devre dışı bırakmayarak zararlı yazılımlara karşı bilgisayarınızı koruma altına alabilirsiniz.

BİLGİSAYAR KULLANICI HESAPLARI VE YETKİ TANIMLAMALARI:

- Bilgisayarlarda yönetici ve standart kullanıcı hesapları bulunmaktadır. Yönetici hesapları bilgisayar içerisinde tam denetime sahip kullanıcıdır. Standart hesaplar ise bilgisayar içerisindeki kurulu yazılımları kullanabilir ve bilgisayar üzerindeki güvenliği etkilemeyecek sistem ayarlarını değiştirebilme yetkisine sahiptir. ***(bakınız: resim-8)***

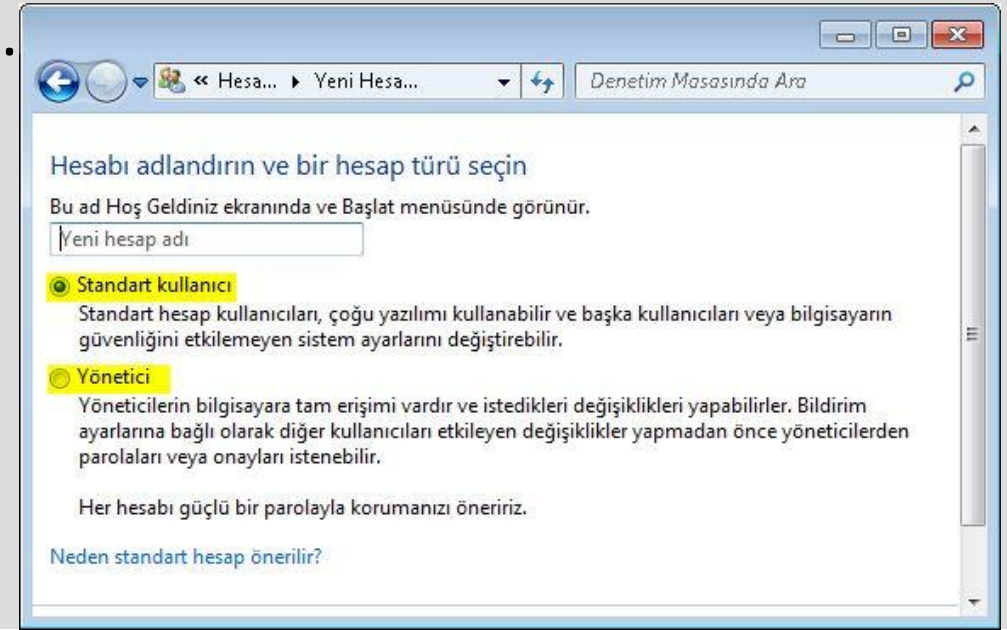


BİLGİSAYAR KULLANICI HESAPLARI VE YETKİ TANIMLAMALARI:

- Bilgisayar içerisinde oluşturulan her bir kullanıcının güvenli şifreye sahip olması gereklidir. Şifresiz kullanıcılarla bilgisayarınız üzerinde ve ağınız üzerinde rahatça işlem yapabilecektir. Bu nedenle her bilgisayar için yönetici hesabı ve standart kullanıcı hesabında iki ayrı kullanıcı yaratılmalıdır ve bu kullanıcıların her birinin şifresi güvenli şifre özelliğinde ve benzersiz olmalıdır.***(bakınız: resim-9 , 9A)***

BİLGİSAYAR KULLANICI HESAPLARI VE YETKİ TANIMLAMALARI:

- Bu sayede bilgisayarınızda yönetici hesabına sahip olmayan kullanıcılar kısıtlı haklara sahip olacağından, yetkisiz erişim ve program kurulumu yapamayacaktır. Ağınız üzerindeki paylaşımlarda, everyone kullanıcı özelliği kaldırılarak, bilgisayar içeriğinde oluşturulan kullanıcılar yetkilendirilerek paylaşılan klasörler içerisindeki datalarınızın güvenliği sağlanmış olacaktır. Bu sayede hem bilgisayarınızı, hem de ağınızı yetkisiz girişlere kapamış olursunuz.



E-POSTA GÜVENLİĞİ

- Elektronik postalarımıza her gün birçok mail gelmektedir. Postalar içerisinde işimizle alakalı postalar ve reklam, banka ekstresi gibi mailler posta kutumuza ulaşmaktadır. Mail sağlayıcılar, genellikle güvenilir mailleri posta kutumuzun gelen kutusuna iletmekte, bilinmeyen onaylanmamış bir adresten gelenleri ise önemsiz, spam klasörüne taşımaktadır. Bazı durumlarda nadir de olsa kaynağı onaylanmamış mailler gelen kutusuna ileti olarak gelmektedir.
- Bu gibi durumlarda maili göndereninin mail adresini, kendimizin doğrulaması çok önem kazanmaktadır. Peki bunu nasıl yapacağız; genellikle banka ekstresi, telefon, adsl fatura detayı ya da kargo detayı olarak karşımıza çıkan bu mailler gönderen mail adreslerinde dikkat ettiğimizde asıl kaynağı tarafından gönderilmediğini anlamamız çokta uzmanlık gerektiren bir durum değildir.

E-POSTA GÜVENLİĞİ

- Genellikle otomatik ödemede bulunan faturalarımız üzerinden bizleri kandırarak bilgisayarlarımıza zararlı yazılımların buluşmasını sağlayan bu maillerden dikkatimiz sayesinde kurtulabiliriz. Günümüzde e-mail üzerinden gelen bu zararlı yazılımlar sürekli form değiştirdiğinden dolayı anti virüs yazılımlarının yakalaması çok kolay olmamakta. Bu gibi durumlarda her ne olursa olsun gönderen mail adresi uzantısına mutlaka dikkat etmeliyiz. Güvenliğinden emin olmadığımız mailleri kesinlikle açmamalıyız. Elektronik posta kutumuzdan açmadan silerek, zararlı yazılımların bilgisayarımıza bulaşma riskinden bilgisayarımızı ve ağımızı korumuş oluruz.

GÜVENLİK DUVARI

- Güvenlik duvarları bilgisayarınız ile internet ağı arasındaki istenmeyen trafiği engelleyen, kontrol altında tutan yazılım ve donanımlardır.

Bu gibi yazılım ve donanımlar ücretli ve ücretsiz olarak bulunmaktadır. Ücretsiz çözümler genellikle Linux , Unix platformlarla gelmektedir. Bu gibi yazılımsal ve donanımsal güvenlik cihazlarının kurulumu orta ve ileri seviyede network ve sistem bilgisi gerektirmektedir.

GÜVENLİK DUVARI

- Aynı zamanda bilgisayarlarınızın işletim sistemleri içerisinde güvenlik duvarları yerleşik olarak bulunmaktadır. İnternete bağlandığınızda bilgisayarın güvenlik duvarı kapalıysa, bilgisayarınız izinsiz erişimlere açık halde demektedir. Zararlı yazılımların, bilgisayarınıza bulaşma riski altında olabilirsiniz. Bu gibi durumlardan, bilgisayarınızın güvenlik duvarını her zaman aktif durumda tutarak kurtulmak mümkündür. Bilgisayar korsanları güvenlik duvarı kapalı olan bir bilgisayarı daha rahat ele geçirebileceklerinden saldırı kaynakları genellikle bu tip bilgisayarlar olmaktadır.

Bilgisayarınıza ,ağınıza ve bilgilerinize ulaşmanın birçok yolu bulunmaktadır. Bu gibi risklerle karşı karşıya kalmamak için güvenlik önerilerini takip etmeli ve uygulamalısınız. Güvenlik önlemleri sayesinde bilgisayarınızı, ağınızı ve bilgilerinizi güvenlik altında tutmanız mümkün olacaktır.

Kaynak: https://www.bilgiguvenligi.gov.tr


TÜRK ECZACILARI BİRLİĞİ
TURKISH PHARMACISTS ASSOCIATION