





Bilgisayarımızın Güvenliđi: Uygulama Dersi


Bilgisayar Güvenliđi Temel Kavramları

 Virüs (Malware): Bilgisayarlara zarar vermek, bilgi çalmak ya da sistemi kullanılamaz hale getirmek amacıyla yazılmış kötü niyetli yazılımlardır. Antivirüs programlarıyla tespit edilip silinmeleri gerekir.

 Spyware (Casus Yazılım): Kullanıcının haberi olmadan bilgisayarda çalışan ve kişisel bilgileri (şifreler, tarama geçmişi vs.) toplayan yazılımlardır. Genellikle ücretsiz programlarla gizlice yüklenir.

 Antivirüs Programı: Bilgisayarı tehditlere karşı tarayan, zararlı yazılımları tespit eden ve gerektiğinde silen koruma yazılımıdır. Gerçek zamanlı koruma özelliđi sayesinde tehditleri anında engelleyebilir. Dosyaları ve yazılımları tarayarak zararlı yazılımları tespit eder ve engeller.

 Güvenlik Duvarı: Bilgisayarınıza gelen ve giden internet trafiđini denetler ve izinsiz bağlantıları engeller.

 Microsoft'un Windows işletim sistemiyle birlikte sunulan güvenlik yazılımıdır. Başlangıçta yalnızca bir antivirüs programı olarak işlev görse de, zamanla daha geniş bir güvenlik çözümü haline gelmiştir. Şu anda Windows 10 ve sonraki sürümlerde, Windows Defender Antivirus ve Windows Defender Güvenlik Duvarı gibi bileşenlerle bilgisayarınızı korur.

Gerçek Zamanlı Koruma: Bir dosya ya da bağlantı açılmadan önce antivirüs tarafından otomatik olarak kontrol edilmesidir. Sistem için ilk savunma hattıdır.

Karantina: Antivirüs programlarının şüpheli dosyaları izole ettiđi güvenli bir alandır. Dosya silinmeden önce incelenebilir, geri yüklenebilir ya da tamamen silinebilir.

1 Tarayıcıda Güvenli Gezinme Ayarları

Uygulama 1: Güvenli Gezinti Açık mı?

Adım 1: Chrome > Ayarlar > "Gizlilik ve Güvenlik" > "Güvenlik" sekmesine gir

Adım 2: "Gelişmiş koruma" veya "Standart koruma" açık mı kontrol et

✓ "Gelişmiş koruma", bilinmeyen tehditlere karşı daha hızlı önlem alır. Herkese önerilir. Açık olmalıdır.

🔗 Uygulama 2: "Do Not Track" Aktif mi?

Adım 1: Chrome > Ayarlar > Gizlilik ve güvenlik > "Üçüncü taraf çerezleri"

Adım 2: "Sitelerin 'Takip Etme' isteğini göndermesine izin ver" seçeneği açık mı?

✅ "Do Not Track" seçeneği aktifse, web sitelerine "beni izleme" sinyali gönderilir. Ancak, bu her zaman etkili olmayabilir, çünkü pek çok site bu sinyale uymamaktadır. Gizlilik açısından önemli bir adımdır, ancak çoğu site bu sinyale uymadığı için, yine de bazı veriler toplanabilir. Bu yüzden, bu özelliği kapalı tutmak daha güvenli olabilir.

🔗 Uygulama 3: Pop-up Engelleyici Açık mı?

Adım 1: Chrome > Ayarlar > Gizlilik ve güvenlik > Site ayarları > "Pop-up'lar ve yönlendirmeler"

Adım 2: "Engelleniyor" (Önerilen) seçeneği aktif mi?

✔️ Pop-up'lar kötü amaçlı yazılımlar için yaygın kullanılan bir yöntemdir. Buna izin vermeyerek, pop-up engelleyiciyi açık tutarak, sitelerin bu tür zararlı öğeler göndermesini engelleyebilirsiniz.

2 Antivirüs Testi – EICAR Dosyasıyla

Hazırlık Notu: Antivirüs programı kurulu olmalı (Windows Defender yeterlidir.) Önlem amacıyla güvenlikten emin olun. Başlat Menüsüne tıklayın ve "Ayarlar"ı açın. "Gizlilik ve Güvenlik" sekmesine tıklayın. "Windows Güvenliği" kısmına tıklayın. Buradan "Güvenlik Duvarı ve Ağ Koruması" seçeneğine tıklayın. Sağ tarafta, "Ağ Profili" seçeneğinin altındaki güvenlik duvarının açık olup olmadığını kontrol edin. Eğer kapalıysa, "Aç" seçeneğine tıklayarak aktif hale getirin.

Adım 1: <https://www.eicar.org/download-anti-malware-testfile/> adresine gidilir

Adım 2: "eicar.com" adlı test dosyasına tıklanır

Adım 3: Antivirüs indirimi engelliyor mu kontrol edilir

✔️ Şimdi kontrol et. Dosya iniyor gibi gözükse bile hemen silinmişse gerçek zamanlı koruma düzgün çalışıyor. İndirilmişse ve indirilenler klasöründe görüyorsan koruma kapalı olabilir. Dosya zararlı olabilir hemen silmelisin ve ayarlarını yeniden kontrol etmelisin.

Şüphe duyduğunuz bir dosya varsa ne yapmalısınız?

Dosyayı manuel olarak tarayın: Zip dosyası olduğunu varsayalım sağ tıklayın ve "Windows Defender ile Tara" seçeneğini seçin.

Eğer başka bir dosya varsa çevrimiçi bir antivirüs aracıyla (virustotal.com gibi) taratabilirsiniz. Böylece birçok farklı antivirüs yazılımı tarafından kontrol edilmiş olur.

3 Gerçek Zamanlı Koruma Açık/Kapalı Testi (Bu adımı denemiyoruz. Zarar verebilir.)

Adım 1: Antivirüs paneli açılır

Adım 2: Gerçek zamanlı koruma devre dışı bırakılır

Adım 3: EICAR dosyası yeniden indirilmeye çalışılır

✓Gerçek zamanlı koruma, ilk savunma hattıdır. Kapalı olduğunda sistem savunmasız kalır.

4 Karantina Süreci – İzleme

Adım 1: Antivirüs paneli açılır (örneğin: Windows Güvenliği > Virüs ve tehdit koruması)

Adım 2: “Koruma geçmişi” veya “Karantinadaki öğeler” sekmesi seçilir

Adım 3: EICAR dosyasının burada listelendiği gözlemlenir

✓Karantinaya alınan dosyalar sistemden izole edilir ama hâlâ mevcuttur.