# ZARARLI YAZILIMLAR

Adem GÜL
Bilişim Teknolojileri Öğretmeni

Bilgisayar sistemlerimize zarar veren, farklı türde birçok yazılım bulunmaktadır. Bu sunu ile onları daha yakından tanıyacağız.

Düşünelim, bir arkadaşımız ya da kardeşimiz hasta oldu ve ondan kısa bir süre sonra hastalık bize bulaştı. Bildiğimiz bulaşıcı hastalıklar üzerinden düşünerek...

**Hastalık nasıl ilerler ya da bulaşır?**
**Hastalıktan vücudumuz nasıl etkilenir?**
**Hastalıktan nasıl kurtuluruz?**

Bilgisayarlar da hastalanır. Bilgisayardaki hastalığa “bilgisayar virüsü” deniyor. Ama genel olarak “Zararlı yazılım” olarak bahsetmek daha uygun.

**Haydi zararlı yazılımlardan ünlü olanlardan bazılarına bakalım ve ortak özellikleri, kendilerine has özellikleri ve zararları ile ilgili düşünelim.**

# ÜNLÜ ZARARLI YAZILIM ve VİRÜS HABERLERİ

# Creeper (1971)

Kayıtlara ilk bilgisayar virüsü olarak geçen Creeper ARPANET'deki bilgisayarlara bulaşmıştır. Bulaştığı bilgisayara herhangi bir zarar vermeyen Creeper asıl zararını, programcıları virüs mantığıyla tanıştırarak vermiştir.

ARPANET : Amerika Savunma Bakanlığı bünyesine bağlı ARPA yani Gelişmiş Savunma Araştırmaları Projeleri Birimi tarafından hazırlanan ilk paket dağıtımı ağı..

# CIH
# Çernobil (1998)

Dünya genelinde yaklaşık 20 ila 80 milyon dolar zarara yol açmış, birçok bilgisayardaki önemli bilgileri yok etmiştir. 1998 yılının haziran ayında Tayvan'da ortaya çıkmış ve çok kısa bir sürede tüm dünyaya yayılmış, Windows işletim sistemindeki hayati dosyalara zarar vermiş ve sistemlerin çökmesine sebep olmuştur. Ayrıca açılış dosyalarına da zarar vermiştir. Bir oyunun demo sürümünün içine de sızan virüs bu demo sürümle de yayılmıştır. Çernobil nükleer santralinin patlaması sonucu çevreye verdiği zarara benzetilmesi sebebi ile de çernobil virüsü diye anılmıştır.

# Melissa (1999)

İlk olarak 26 Mart 1999 yılında görülmüştür.
“İşte aradığınız belge... Bu belgeyi sakın kimseye gösterme ;-)”. Mesajı içeren bir elektronik postada ekli .DOC uzantılı bir kelime işlemci dosyasının açılması ile bulaşan ve otomatik elektronik posta yollayan virüsün 300 ila 600 milyon dolar zarara uğrattığı sanılıyor.
2003 yılından sonraki kelime işlemci programları virüsten etkilenmemiştir.

# I love you (2000)

Loveletter (Aşk mektubu) olarak da bilinen virüs, elektronik postalara eklenen “Love-Letter-For-You.TXT.vbs” adlı programın çalıştırılması ile bulaşmış, elektronik posta uygulamasının adres defterindeki kişilere kendini göndermiştir.  ILOVEYOU virüsünün yaklaşık olarak 10 ila 15 milyar dolar zarara neden olduğu sanılmaktadır.

# Code Red (2001)

Bir bilgisayar worm'u olarak bilinen ve ağ sunucuları üzerinde yayılan Code Red, ilk olarak 2001 yılında görüldü. Oldukça tehlikeli olan bu solucanın amacı ise web sunucusunun zayıf noktalarını tespit edip zarar vermekti. Bady ismiyle de bilinen Code Red, sunucunun web sayfalarında ise şu mesajı yayınlamıştır.

**"HELLO! Welcome to http://www.worm.com! Hacked by Chinese!"**.

400.000 kadar sunucuyu etkilediği sanılan Code Red, kısa sürede bir milyondan fazla bilgisayara sızmayı başarmıştır.

# Bagle (2004)

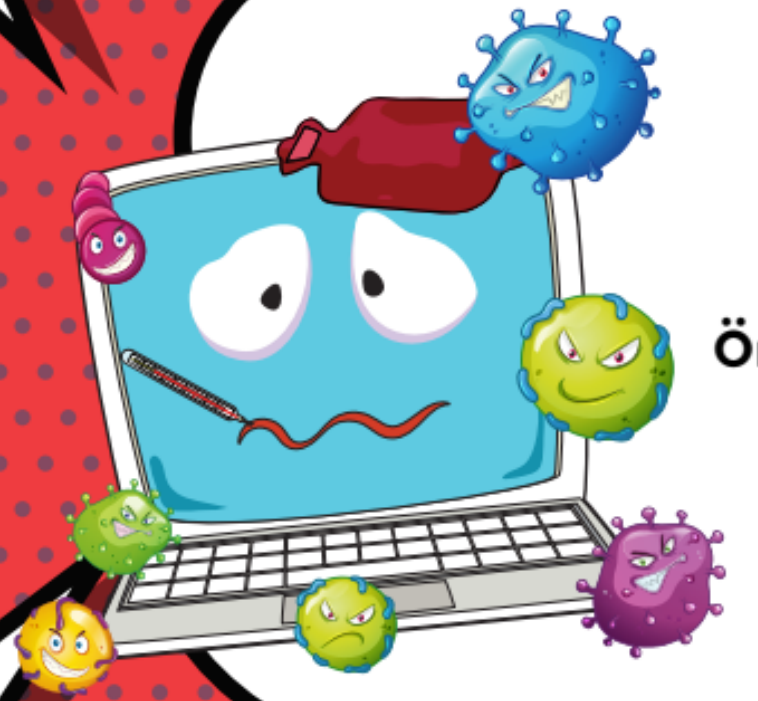
On milyonlarca dolar zarara neden olan ve sayısız PC'ye sızmayı başaran Bagle, 8 Ocak 2004 tarihinde ilk kez görülmüş, Bagle, elektronik postalardaki dosyaları kullanarak yayılmaya çalışmıştır. Bagle'ın en kötü tarafı 60 ila 100 kadar türevinin olmasıydı. Diğer bir deyişle Bagle'ın virüs tarayıcılara yakalanması pek kolay değildi. PC'lere sızan Bagle, veri ve uygulamalara kolayca ulaşabiliyordu. Finansal ve kişisel bilgiler dahil hemen her veriye eli uzanabilen Bagle'ın Bagle.B türevinin yayılması 28 Ocak 2004 tarihinden itibaren durduruldu, ancak Bagle'ın diğer türevleri hâla tehdit unsuru olmayı sürdürüyor.

# Sasser (2004)

30 Nisan 2004 tarihinde görülen Sasser, havayolu şirketlerine kadar ulaşmış uçuşların ertelenmesine sebep olmuştur.  Klasik solucanların aksine, elektronik postaları kullanmayan Sasser, güncel olmayan işletim sistemlerinin güvenlik açıklarını kullanmıştır. 17 yaşındaki bir Alman lise öğrencisi tarafından yazılan ve 18. yaş gününde yaymaya başladığı Sasser'ın yarattığı zarar öylesine büyük oldu ki bu Alman genci bilgisayarlara karşı sabotajda bulunduğundan dolayı hapis cezasına mahkûm edildi.

# (2013)
# CryptoLocker

CryptoLocker, fidye isteyen kategoride (ransomware) bir zararlı yazılımdır. Virüs, şifrelediği her bir klasöre ve kullanıcı masaüstüne “SIFRE_COZME_TALIMATI.html” benzeri bir dosya eklemektedir. Bu web sayfası şeklindeki dosya bilgisayardaki dosyaların özel bir program ile şifrelendiğini, dosyaları kurtarmanın tek yolunun şifre çözen programı satın almak olduğunu belirtmiştir. Virüsün dosyaları şifrelemesi durumunda, yapılabilecek çok fazla seçenek bulunmadığından önemli olan husus virüsün bulaşmasını engellemektir. Ülkemizi de etkileyen bir virüstür.



Haberlerden yola çıkarak
şu sorulara yanıt verelim.

**Virüslerin amacı nedir?**
**Örneklere ve deneyimlerimize göre virüsler ne gibi zararlar verirler?**

Zararlı yazılımlar; amaçları, bulaşma şekilleri, verdikleri zararların boyutları gibi birçok ölçüte göre gruplanabilmektedir.

Bilgisayarınızdaki bilgileri çalabilir ve başkalarına gönderebilirler

- E-posta hesaplarınız, parola bilgileriniz gibi.

İşletim sisteminizin veya diğer programlarınızın

- çalışmamasına,
- hatalı çalışmasına neden olabilirler.

Bilgisayarınızdaki dosya veya klasörleri

- silebilir,
- kopyalayabilir,
- yerlerini değiştirebilir veya yeni dosyalar ekleyebilirler.

Yaptığınız her şeyi kaydedebilirler.

- Klavyede yazdığınız her şey veya fare ile yaptığımız tüm hareketler gibi.

Ekranda can sıkıcı veya kötü amaçlı web sitelerine yönlendiren açılır pencereler oluşturabilirler.

Tüm verisiyle diski silebilir, hatta biçimlendirebilirler.

Saldırganların kullanması için güvenlik açıklıkları oluşturabilirler.

Başka zararlı programların bulaşmasını sağlayabilirler.

Bilgisayarınız üzerinden başkalarına saldırabilirler.

Bilgisayarınızın ya da internetin kaynaklarını kullanır, yavaşlamalara neden olabilirler.

# ZARARLI YAZILIM TAYFASI

**Ben bir Virüs'üm!**
Çoğalırım, başka programın içinde yaşarım, bulaşırım. Bilgisayarı yavaşlatırım, bilgileri bozabilirim.

**Ben bir Trojan'ım!**
Saklı dururum, zarar vermem, zor farkedilirim. İndirilen bir oyunun içinde gizlenerek bulaşır, bilgileri sessizce çalarım.

**Ben bir Solucan'ım!**
Başka programa ihtiyacım yok, ağdan bulaşıp, ağda gezerim.

**Ben bir Rootkit'im!**
Bilgisayarları uzaktan kullanırım.

Keylogger

Tüm klavye hareketlerini kaydederim ve gizlice gönderirim. Tüm yazışmaları, gezinmelerinizi, parola ve kart bilgileri gibi bilgilerinizi ele geçirebilirim.

**Ben bir antivirüs yazılımıyım.**

Zararlı yazılımları tanırım, bilgisayarınızda bulursam silerim, silemezsem karantinaya alırım, yeni virüsleri takip ederim, izinsiz girişleri engellerim, sistemi hızlandırmaya çalışırım.

# Virüsleri Nasıl Fark Ederiz ve Virüslerden Nasıl Korunuruz?

1. Sistem **yavaşlarsa**
2. Bilgiler **kayboluyorsa**
3. **İstenmeyen** programlar, internet sayfaları **açılıyorsa**
4. Bilgisayar **verdiğiniz komutları yerine getirmiyorsa**
5. Bilgisayar **isteğiniz dışında işlem yapıyorsa**
6. Bazı **dosyalar açılmıyorsa**

**bilgisayarınıza zararlı yazılım BULAŞMIŞ OLABİLİR!**

**Zararlı yazılımlardan korunmak ve zararı en aza indirmek için**

1. Güvenlik duvarı kullanın,
2. Önemli bilgilerinizi yedekleyin,
3. İşletim sistemlerini güncelleyin, Bazı işletim sistemleri daha güvenlidir UNUTMAYIN,
4. Virüs/yazılım koruma programları kullanın, programları güncelleyin,
5. Emin olmadığınız elektronik posta eklerini açmayın,
6. Güvenilir olmayan sitelerden program/müzik/oyun indirmeyin,
7. Tarayıcının güvenlik ayarlarını üst düzeyde tutun,
8. Aynı anda birden fazla antivirüs programı kurmayın,
9. Bulaşmış virüsü temizleyemiyorsanız başka antivirüs yazılımlarını deneyin veya işletim sistemini biçimlendirin.

# KORUYUCU YAZILIMLAR VE KULLANIM AMAÇLARI

# GÜVENLİK DUVARLARI

Güvenlik duvarı bilgisayarımızın veri trafiğini kontrol eden bir yazılım ya da donanımdır. Güvenlik duvarı kullanmak en temel koruma yöntemlerindendir. Bazı işletim sistemlerinde güvenlik duvarı uygulaması işletim sistemi ile gelmektedir. Uygulama cihazınızı yavaşlatsa dâhi, uygulamayı durdurmamak ve güncellemek önemlidir. Çünkü bu yazılımlar, yetkisiz kullanıcıların ve solucanların bilgisayara girişini engelleyip istenmeyen trafiği engelleyerek bilgisayarları korur. Güvenlik duvarı sadece bireysel kullanıcılar tarafından değil daha gelişmiş güvenlik önlemlerine ihtiyacı olan kurumlar tarafından da kullanılır.

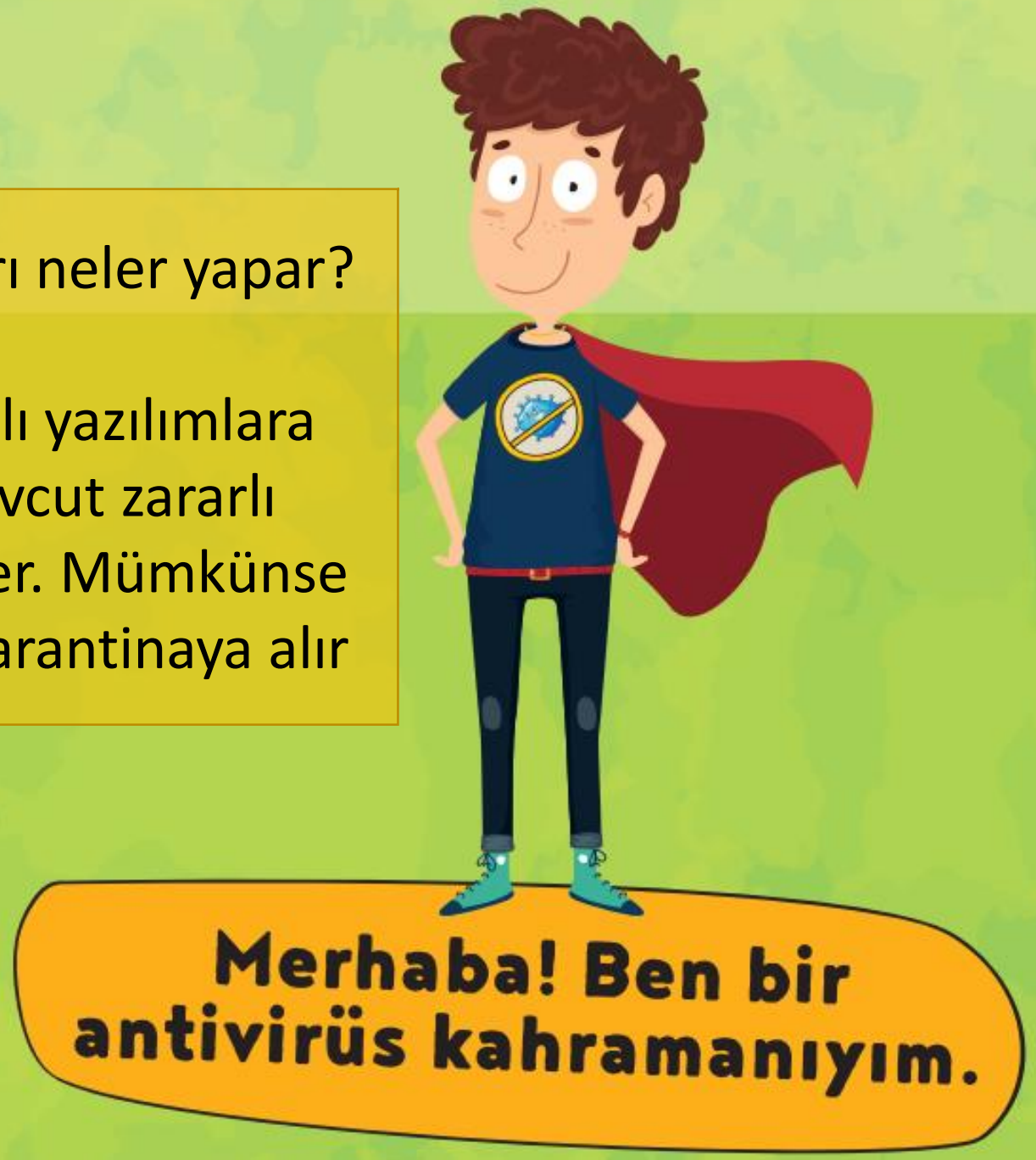
# ANTİVİRÜS

Antivirüs yazılımı bilgisayarımıza virüs, truva atı, solucan gibi kötü amaçlı yazılımların girmesini engeller. Ayrıca bu yazılımları tespit edip temizleyebilir.

Antivirüs yazılımının tüm kötü yazılımları tanıyabilmesi için sürekli güncelleştirilmesi gerekir.

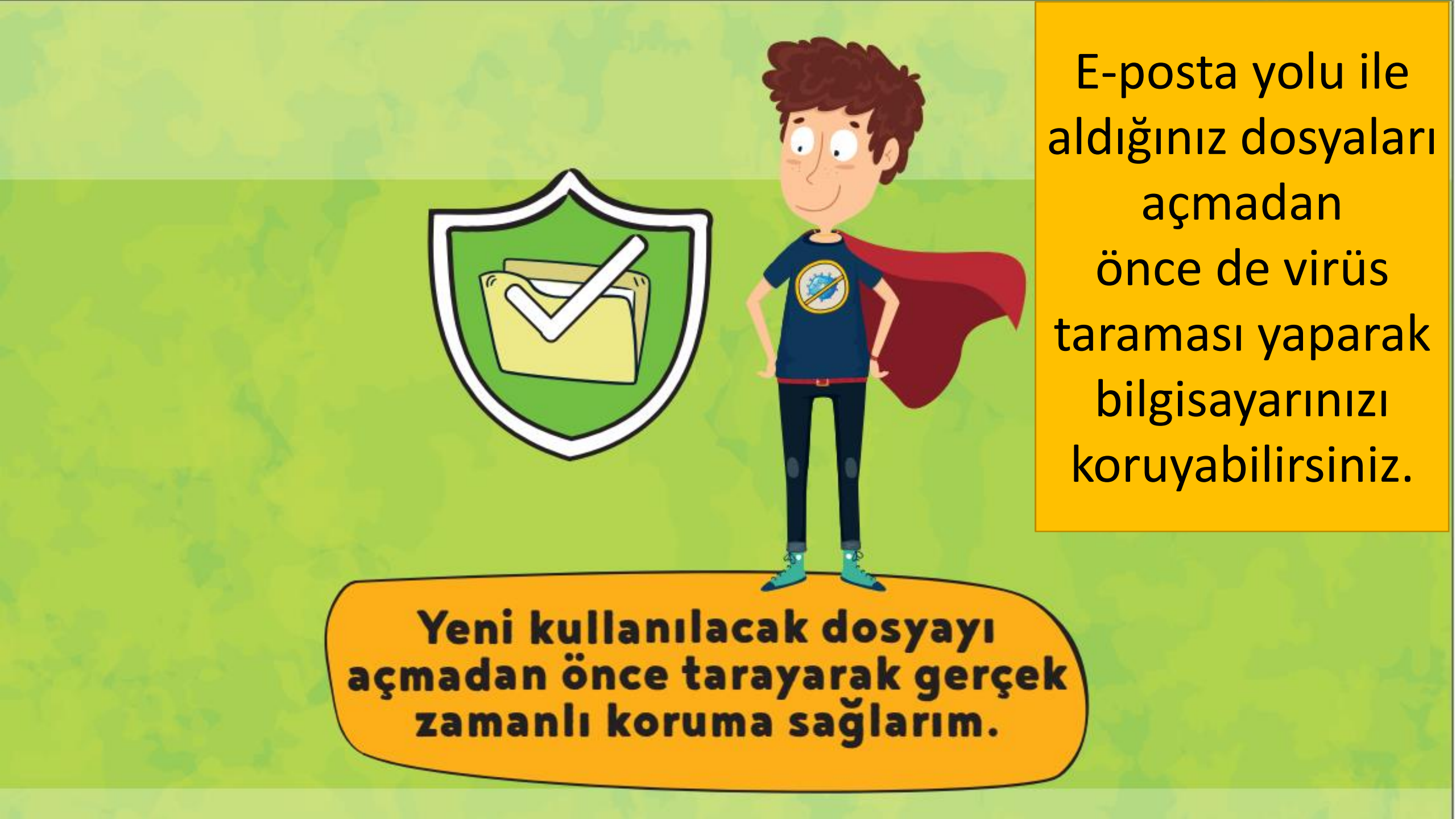
Antivirüs programları neler yapar?

Bilgisayarınızı zararlı yazılımlara karşı korur ve mevcut zararlı yazılımları tespit eder. Mümkünse siler, silemezse de karantinaya alır



Bazı virüsler dosyalara da bulaşır. Antivirüs programları virüslerin dosyalarınıza bulaşmasını engeller


Başkasına ait taşınabilir bir belleği bilgisayara takmadan önce virüs taraması yapmak önemlidir. Tarama sonucu her zaman zararlı yazılımı bulamayabilir. Çünkü, antivirüs programları tüm virüsleri tanımayabilir. Virüsleri temizlemek için virüslerin antivirüs programlarında tanımlı olmaları gerekir. Güncelleme ile Antivirüs programlarının etki alanı genişletilebilir.




E-posta yolu ile aldığınız dosyaları açmadan önce de virüs taraması yaparak bilgisayarınızı koruyabilirsiniz.


İnternette gezinirken, siber saldırıya uğrayabilirsiniz. Antivirüs programları; gizliliği arttırarak internette gezinmenizi güvenli hâle getirmeye, bunu yaparken de bilgisayar performansını üst seviyede utmaya çalışır.


İnternette en sık karşılaşılan sorunlardan biri istemediğiniz bir sayfada gezinirken istemsiz başka bir sayfaya yönlendirilmek ve gezinmeyi engelleyecek reklamların açılmasıdır. Antivirüs programları bu durumlarla da mücadele etmeye çalışır.

Parola bilgilerinizi güvenli tutabileceğiniz araçlar sunarım.

Kapsamlı güvenlik durumu raporlaması sağlarım.

*Kötü amaçlı eylemleri sonlandırmanızı sağlar bazen zararlı yazılımların verdiği zararları geri almaya çalışır. Bozulan içeriğin onarılması buna bir örnektir.*

Akıllı İşaret (kare barkodlar, kare kodlar) bağlantısının güvenliğini denetlerim.

Cep telefonunuzu da zararlı yazılımlardan koruyabilirim.

Kesintisiz bir şekilde uygulamalarınızı kullanmanıza yardımcı olurum.


*Sonuç olarak, antivirüs programları cihazlarımızı korumamızda çok önemli yardımcılardır. İşlerini daha iyi yapabilmeleri için sıkça güncellenmeleri gerekir. Güvenli sitelerden elde edilmeyen Antivirüs yazılımlarının bile virüs içerebileceğini unutmayalım.*