



ONDOKUZ MAYIS ÜNİVERSİTESİ
UZAKTAN EĞİTİM MERKEZİ

Çağrı Merkezi Hizmetleri Önlisans Programı

Bilgi ve İletişim Teknolojileri

Öğr. Gör. Muhammed KARA

Fırsatlar Sunar



Ünite 4

BİLGİSAYAR VE İNTERNETTE GÜVENLİK VE GÜVENLİK ARAÇLARI

Öğr. Gör. Muhammed KARA

İÇİNDEKİLER

4.1. VİRÜS NEDİR?.....	3
4.1.1. Virüs Çeşitleri:.....	3
4.1.2. Bilgisayar Virüslerinin Olası Zararları Nelerdir?	3
4.1.3. İnternet Ve Bilgisayar Güvenliği İçin Temel Önlemler	3
4.1.4. Sonuç:.....	7
4.2. KAYNAKÇA	8

4.1. VİRÜS NEDİR?

Bir bilgisayar virüsü,

- Belleğe Yerleşen,
- Çalıştırılabilen Programlara Kendini Ekleyen,
- Yerleştiği Programların Yapısını Değiştiren, Kendi Kendini Çoğaltabilen kötü amaçlı programlardır.

4.1.1. Virüs Çeşitleri:

- Açılış “boot” sektörü virüsleri
- Dosya virüsleri
- Sistem Virüsleri
- Makro virüsleri (Word, excel..)
- Kütük tipi virüsler; (.com, .exe, .bat)
- Truva Atları (oyun, uygulama,..)
- Bilgisayar Kurtları (Solucan)

4.1.2. Bilgisayar Virüslerinin Olası Zararları Nelerdir?

Bilgisayar virüsleri,

- Ekranınıza can sıkıcı mesajlar çıkararak çalışmanızı bölebilir/engelleyebilir.
- Bilgisayarınızın hafızasını ve/veya disk alanını kullanarak bu kaynaklara verimli olarak erişiminizi engelleyebilir.
- Kullandığınız dosyaların içeriklerini bozabilir/silebilir.
- Kullandığınız bilgisayar programlarını bozabilir, çalışmalarını yavaşlatabilir.
- Sabit diskinizin tamamını ya da önemli dosyaların olduğu kısımlarını silebilir.

4.1.3. İnternet Ve Bilgisayar Güvenliği İçin Temel Önlemler

Günümüzde, dünyada 400 milyon civarında İnternet’e bağlı bilgisayar, 1 milyarı aşkın İnternet kullanıcısı, 100 milyona yakın web sitesi olduğu tahmin ediliyor. Türkiye açısından bakıldığında bu rakam 15 milyona ulaşmış durumda; buradan İnternetin, olmazsa olmazlarımızın içine girmiş olduğunu çıkarabiliriz. İnternet’i kullanarak birçok işimizi halletmekteyiz; Örneğin e-posta yoluyla iletişim, bankacılık işlemleri, bir dosyayı karşıdan yükleme, bir ürün hakkında bilgi edinme, iş başvurusu yapma gibi pek çok amaç için kullanmaktayız. Bu büyük platformda, uygulamaları kullanırken kendi kişisel bilgilerimizi (kredi kartı numaramız,e-posta şifre veya kullanıcı adımız, özlük bilgilerimiz vs..) ortama sunmak durumunda kalıyoruz veya net üzerinden dosya,mail vb.. karşıdan yüklemelerimiz oluyor. Bu durumlarda güvenlik açısından önlemler almamız gerekir çünkü İnternet ortamında casus yazılımlar veya kimlik bilgilerinizin çalınması, kullanılmaya çalışılması gibi durumlarla karşı karşıya kalma ihtimalimiz oldukça yüksek. Bu önlemleri geniş bir şemsiye altında parçalara bölerek inceleyelim:

Bu duruma belki de İnternet'te en yaygın olarak kullandığımız veya ihtiyaç duyduğumuz teknoloji diyebiliriz. Dünya'nın öbür ucundan bir dosyayı (müzik,film..) veya gelen bir e-postayı (excel,powerpoint veya bir rar dosyası), sizin kendi bilgisayarınıza, İnternet'i kullanarak indirebilmenizdir.Peki bu kadar sıklıkla kullandığımız bu durumu güvence altına nasıl alacağız? Çeşitli yöntemler;

4.1.3.1. Güncel Antivirüs Yazılımı Kullanımı

4.1.3.1.1. Antivirüs Programları



4.1.3.1.2. Antivirüs Programı Nedir Ve Ne Yapar?

Malware (virusler,solucanlar,truva atları,casus yazılımlar..) gibi bilgisayara ve kullanıcıya (kullanıcı verileri,dosyaları..) ciddi zararlar verebilecek olan yazılımları saptama,silme ve bilgisayarı koruma en temel görevleri olup, aynı zamanda sürekli aktif halde çalışabilen ve güncellenmesi gereken yazılımlardır.

4.1.3.1.3. Antivirüs Programları Neden Güncellenmelidir?

İnternet'te çok ciddi sayıda casus yazılımlar, solucanlar, keyloggerlar vs.. bulunmakta ve daha bilmediğimiz pek çok çeşit de ortaya çıkmaya devam edecek gibi görünüyor. Nasıl bilgisayarımız (işletim sistemimiz) sürekli güncellenmek durumundaysa aynı şekilde antivirüs programımızı da güncellemek durumundayız. Bunun nedeni zararlı yazılımların da günden güne gelişmesi ve antivirüs programlarını rahatlıkla aşabilecek duruma gelmesidir. Bu açıdan antivirüs programımızın güncellenme özelliği her zaman açık olmalı ve belirli aralıklarla, olaylara bağlı olarak bilgisayarımızı taratmalıyız. Son olarak ve en önemlisi de, antivirüs programımızı asla kapatmamalıyız.

***Tüm gelen dosyalar veya e-posta yoluyla gelmiş olan ekleri antivirüs programımızı kullanarak taramak.**

Bütün antivirüs programlarının bu özelliği vardır ve temel sayılabilecek bir özelliktir. Bizim karşından yüklediğimiz veya yükleyeceğimiz öğeyi, dosyayı.. virus taramasından geçirmemiz de fayda vardır.

4.1.3.2. Kişisel Güvenlik Duvarı Kullanımı

4.1.3.2.1. Güvenlik Duvarı Nedir?

İnternet güvenlik duvarı, İnternet üzerinden bilgisayarınıza erişmeye çalışan bilgisayar korsanlarını, virüsleri ve solucanları engellemeye yardımcı olan yazılım kodu parçası veya donanımdır.

4.1.3.2.2. Güvenlik Duvarı Neden Kullanılmalı?

İnternete bağlandığımızda bilgisayarımızın güvenlik duvarı kapalıysa, bilgisayar korsanlarına bilgisayarımıza erişim hakkı ve bilgi almaları için bir davetiye çıkarmışız demektir. Bir başka açıdan bakalım, herhangi bir İnternet sitesine girdiğimizde sayfanın nasıl uygulamalar çalıştırdığını bilemeyiz; Eğer güvenlik duvarımız aktif durumda değil ise bu durum bizi sıkıntıya sokabilir. İnternetinizi güvenlik duvarı olmadan kullanmak, evinizden dışarı çıkarırken evinizin kapısını açık bırakıp gitmeye benziyor; girip çıkabilirsiniz fakat saldırıya çok açık durumundasınızdır. Bilgisayar korsanları özellikle güvenlik duvarı kullanmayan insanları hedefliyor ve bulabilmek için çeşitli yazılımlar geliştiriyorlar. (trojan, solucan, virüs..) Bu açıdan güvenlik duvarı kullanmanın önemi büyük.

4.1.3.2.3. Güvenlik Duvarı Nasıl Çalışır?

Güvenlik duvarı aktif olduğu durumda ağ üzerindeki tüm bağlantıları izler ve tüm trafiği kontrol eder. İstenmeyen bir bağlantı olduğunda o bağlantıya ait trafiği keser, güvenliğini sağlar. Güvenlik duvarları dinamik olarak da çalışırlar. Bazı durumlarda bağlantıyı dinamik olarak açar, erişmek istediğimiz web adresine direk bizi ulaştırırlar. (Bağlantı noktası, bir ağ trafiği türünün bilgisayarınıza eriştiği noktayı tanımlayan, ağ konusuna yönelik bir terimdir. Açtığınız bağlantı noktaları göndermek ve almak istediğiniz trafik türüne bağlıdır.)

4.1.3.3. İşletim Sistemleri Güncelleştirmeleri

4.1.3.3.1. İşletim Sistemi Nedir?

Özetle işletim sistemi, bilgisayarların çalışabilmesi için gereken temel yazılımdır. Bilgisayarlar, çeşitli donanım ürünlerinin belli bir tasarıma göre bir araya getirilmesiyle oluşturulur. Bilgisayarda yaptığımız çalışmaları, internet kullanımını ve bunlar gibi birçok uygulamayı gerçekleştirdiğimiz sanal platform diyebiliriz.

4.1.3.3.2. İşletim Sisteminin Güncellenmesi Neden Önemlidir?

İşletim sistemleri, %100 kararlı yapılardır. Bugünlerde bilgisayar teknolojisi sürekli değişen bir ivmeyle artar durumda ve işletim sistemleri bu mekanizmanın en temel yapı taşlarından biri. Güvenlik açısından baktığımızda önemi daha da artıyor çünkü güncellemelerin birçoğu da güvenlik bazlı oluyor. Güvenlik ve diğer güncellemeler, virüslere, solucanlara, truva atlarına vs.. karşı geliştirilen yapılar olup; bilgisayarımızı teknolojinin hızına entegre edip aynı zamanda güvenliğimizi kontrol altında tutmayı amaçlıyor.

4.1.3.4. E-Posta Konusunda Dikkat Edilmesi Gereken Hususlar

Posta filtresi: Çoğu mail programı istenmeyen maillerinizi filtrelemeyi ve ayrı bir yere çıkartmayı sağlıyor. (e-posta filtre güncelleştirmelerine dikkat etmekte fayda var)

İnternet çok büyük ve gelişmiş bir yapı oldu. Bu yapının içerisinde insanlar birbirleriyle sürekli iletişim halinde. Bu sonuç bilgisayar korsanlarının ekmeğine yağ süren cinsten çünkü iletişimin rahat olması onlar için ciddi bir avantaj haline geliyor.

Bu nasıl oluyor?

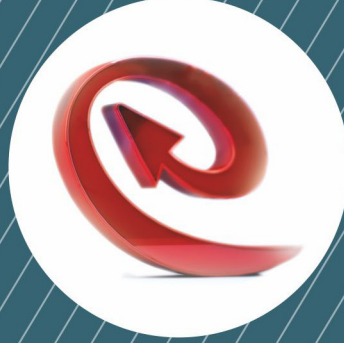
E-postalarımıza hergün birçok posta geliyor, bazıları işimizle alakalı, bazıları özel hayatımızla alakalı, bazıları reklam olan iletiler alıyoruz ve cevaplıyoruz. Peki aldığımız ve kimden geldiğini bilmediğimiz postaların hepsi güvenilir mi? Güvenliğinden emin olmadığımız iletileri açmadan silmekte fayda var çünkü açtığımız anda o dosya, bilgisayarımızı tehdit altında bırakır. Sadece bilgisayarımızda değil, e-posta hesabımızdaki bilgiler, hesaplar ciddi zararlar görebilir. Bu nedenle tanımadığımız postaları direk olarak silmek gerekir. Yine aynı şekilde bilmediğimiz bir adresten posta yoluyla gelen resim, müzik vb. dosyalarını da açmamak ve bilgisayarımıza kurmamak gerekiyor, çünkü resimler zararlı kod içerebilir ve filtrelelere rağmen istenmeyen posta, gönderenin iletisini kullanıcıya ulaştırmak için kullanılabilir.

4.1.4. Sonuç:

Görüldüğü üzere bilgisayarımıza veya bilgilerimize korsanlarının ulaşmaları için birçok yöntem var ve bunlar sürekli olarak gelişme göstermektedir. Bu açıdan güvenlik, kesinlikle küçümsememesi gereken ve önlemler alınması gereken bir konu. Bunun için güvenlik yazılımları, önlemleri, bilgilendirmesi gibi birçok yöntem oluşmuş durumda ve günden güne geliştirilmekte. Bizlere tek ve basit görev düşmekte; Bu güvenlik önlemlerini dikkate alıp, e-postalar, web siteleri, banka hesapları vb. gibi İnternet üzerindeki tüm uygulamalarda gerekli güvenlik önlemlerini almak. Umarız birgün İnternet teknolojileri yapısı kökten ciddi bir evrime uğrar ve bilgisayar korsanlığı veya dolandırıcılığı gibi şeyler bu ortamda barınamaz, kendimizi güvende hissederiz.

4.2. KAYNAKÇA

- <https://tr.wikipedia.org/>
- Öğretim elemanı ders notları
- Megep modülü ders notları
- <https://www.bilgiguvenligi.gov.tr/son-kullanici-kategorisi/internet-ve-bilgisayar-guvenligi-icin-temel-onlemler.html>



Ondokuz Mayıs Üniversitesi Uzaktan Eğitim Merkezi
Kurupelit Kampüsü Atakum / SAMSUN



0362. 457 8936 **Fax:** 0362. 457 5806



irtibat@uzem.omu.edu.tr



<http://uzem.omu.edu.tr>