*Bu broşürde **Bilgi ve Bilgisayar Güvenliği: CASUS YAZILIMLAR ve KORUNMA YÖNTEMLERİ** adlı kitabın tanıtımı sunulmaktadır.*

## GÜVENLİK İLE İLGİLİ EN KAPSAMLI KİTAP ÇIKTI!

Bilgisayar ve İnternet kullanımı sırasında çok büyük maddi ve manevi zararlara uğramak mümkündür.

Sanal âlemin getirebileceği zararlar, ne yazık ki sanal değil gerçektir. Bilinçli bilgisayar ve İnternet kullanımı, her açıdan çok önemlidir. Bunun için, **B**ilgi ve **B**ilgisayar **G**üvenliğinin (BBG) kapsamlı bir şekilde öğrenilmesi ve bilinçlenmek şarttır. BBG, bu konudaki açığı kapatacak kapsamlı bir kaynak olarak; merak ettiğiniz konuları açığa çıkartacak ve bilmediğiniz birçok konuyu gün yüzüne çıkartacak bir kitaptır.

## KİTABIN HEDEF KİTLESI

- Bilgi ve Bilgisayar güvenliğine önem verenler
- Bilişim teknolojileri yöneticileri
- Bilgisayar mühendisleri ve programcıları
- Üniversite öğrencileri
- Sistem ve ağ yöneticileri
- Web tasarımcıları
- Öğretmenler
- İşyeri yöneticileri
- Ebeveynler
- Öğretim elemanları ve
- Minimum güvenlik riski ile bilişim teknolojilerinden maksimum verim almak isteyen her düzeyde bilgisayar kullanıcısı


BBG

Bilgi ve Bilgisayar Güvenliği

Tanıtım İnternet Adresi:
http://www.canbek.com/BBG

Kitap sipariş/istek:
kitap@canbek.com

# BİLGİ ve BİLGİSAYAR GÜVENLİĞİ: CASUS YAZILIMLAR VE KORUNMA YÖNTEMLERİ

*Güvenliğinizi şimdiden temin edin!*
*Yarın çok geç olabilir...*

# KİTAPTAN BAŞLIKLAR

**Bilgi ve Bilgisayar Güvenliği: CASUS YAZILIMLAR VE KORUNMA** yöntemleri kitabında ele alınan başlıkların bir kısmı:

- Dünden bugüne, tarihi ve modern şifreleme yöntemleri
- Bilginin kapsamı ve önemi
- Veri, bilgi, özbilgi ve hikmet: Bilgi çağının merdiveni nedir?
- Bilgi ve bilgisayar güvenliği ve unsurları
- Bilgi güvenliği risk yönetimi ve güvenlik süreçleri
- Siber uzayın gelişimi
- Bilişim korsanlığı (hacker) ve kültürü
- Beyaz ve kara şapkalı korsanlar, betik kerataları (script kiddy), tıklama kerataları (click kiddy), (sistem) kırıcılar (cracker), web sitesi tahrifatçıları, korsanlık hareketi (hactivizm)
- Siber terörizm (cyber-terrorism) ve siber savaş (cyberwar) ya da bilgi savaşları
- Dünya ve Türkiye'den gerçekleşmiş önemli siber uzay olayları
- Dünya ve Türkiye'den bilişim korsanları
- Bilgisayar sistemlerine yapılan saldırılar ve türleri
- Saldırı tehdit karakteristikleri ve saldırgan profili
- Sosyal Mühendislik ve insan hatası
- Kişisel gizlilik (mahremiyet, privacy) ve boyutları
- Bilişim suçları (cybercrime)
- Ülkemizde bilişim suçlarına yönelik yasal düzenlemeler
- Kötücül yazılımlar (malware) ve bütün çeşitleri
- Klavye dinleme sistemleri (keylogger)
- Casus yazılımların (spyware) ortaya çıkışı ve gelişimi
- Casus yazılımlara karşı alınabilecek önlemler
- Casus savar yazılımları (antispyware)
- En son kötücül ve casus yazılım vakaları
- Casus yazılımların "müşteri" (kurban) çekme teknikleri
- Casus yazılımların yumuşak karnı: Otomatik başlatma yöntemleri
- Çocuk ve gençleri siber uzayda bekleyen tehlikeler ve çocuklarımızın bilgisayar ve İnternet güvenliği
- İşyerinde verimliliğin ve güvenliğin artırılması
- İşyerinde elektronik gözetleme

## SAYILARLA KİTAP

BBG kitabı ile ilgili aşağıdaki istatistikler kitabın taşıdığı değeri göstermek için aşağıda sunulmuştur:

**HACİMLİ!**

Sayfa sayısı: 504

**KAPSAMLI!**

Bölüm sayısı: 22

**AYRINTILI!**

Alt Başlık sayısı: 234
Dizin anahtar sözcük sayısı: 888

**ZENGİN GÖRSEL İÇERİK!**

Çoğu özgün şekil/resim/fotoğraf sayısı: 255

**ZENGİN GÜNCEL VERİ!**

Çizelge/tablo sayısı: 32

**BİLİMSEL VE YÖNELTİCİ!**

Kaynak/atıf sayısı: 435

## TANITIM

Bilgi çağında yaşıyoruz! Dünyanın en büyük kütüphanesi olan Amerikan, Kongre Kütüphanesinde var olan basılı koleksiyonun tamamının 10 tera bayt'lık (~10.000 GB) bir bilgi kapasitesinde olduğu düşünülürse; sadece 2002 yılında üretilip depolanan yeni bilgi, 100.000 Amerikan Kongresi Kütüphanesindeki bilgiye denk düşmektedir. Bilgi çağında bilişim teknolojilerinin geldiği nokta baş döndürücüdür. 2002 yılında 18 eksabayt'lık ($18 \times 10^9$ GB) yeni bilgi, telefon, radyo, televizyon ve İnternet aracılığıyla taşınmıştır. Dünya nüfusunun %15,7'si (1.023 milyon kişi) İnternet kullanmaktadır.

Bilgi, en basit benzetme ile para gibi bir metadır. Kişiler, kurumlar ve ülkeler için bilgi, elde edilmesi zor; aynı zamanda elde tutulması da zor olan bir metadır. Fikri mülk olarak tanımlanan bu meta, bir kurumun bilgi ve özbilgi (knowledge) varlığıdır. Bu mülkün korunması, hayati bir önem arz etmektedir. Bu önem, tarihteki en eski uygarlıklardan günümüze kadar devam etmiştir. Şifreleme, bilgi güvenliğinin en eski uygulamaları arasında yer almış; bilgisayar güvenliğinin en önemli unsurlarından biri olan gizliliğin temini için teknolojinin yardımı ile gelişmiştir.

Siber uzay ya da siber âlem, artık bir bilim kurgu ütopyası olmaktan çıkmıştır. Dalgalar, elektrik yükleri ve manyetik durumlar olarak, elektromanyetik tayfta bulunan, elle tutunamayan veri ve yazılımlar olarak tanımlanan siber uzayın varlıkları, fiziksel olarak telefon, radyo, televizyon, bilgisayar, veri depolama cihazları, yazıcılar, ağ kabloları, cep telefonları ve uydularda bulunmaktadır. İnternet (Genel ağ), siber uzayın en büyük, en kapsamlı ve en etkili bileşenidir. Ama İnternet dışında; İntranet, diğer özel bilgisayar ağları, telefon şebekeleri, GSM hücreleri, haberleşme ve GPS uydu ağı gibi ağlar da siber uzayın içindedir.

Kişisel gelişimi ve verimliliği sağlamak, bilim ve teknolojide ilerlemek, şirketlerin karlılığını ve üretimini artırmak için bilginin öneminin kavranılması; bilgiye erişimin hızlanması ve kolaylaşması ve var olan veya elde edilmiş olan bilginin korunması şarttır.

Bilişim teknolojilerinin nimetlerinden özgürce ve istenildiği gibi yararlandığımız şu günlerde, insanlar ve kurumlar çok önemli tehdit ve risklerle karşı karşıyadır. Bilgisayarlar ve İnternet kullanımının hızla arttığı böyle bir ortamda, çeşitli sebeplerle bilgi ve bilgisayar güvenliği göz ardı edilmektedir.

Siber uzayda, yeterli bilgi birikimi ve deneyime sahip olmayan kullanıcılar, insan ve kuruluşlara maddi ve manevi açıdan çeşitli düzeyde zararlara uğratmak için uğraşan genelde kara şapkalı "bilişim korsanı" ya da "hacker" olarak adlandırılan kötü niyetli kişilerin tuzaklarına çok kolay bir şekilde düşebilmektedir. Sanal ortamda, bu durumda oluşan zarar, ne yazık ki "sanal" olmamaktadır. Yeterli güvenlik önlemlerini almamış kişiler, kredi kartı bilgileri gibi önemli bilgilerin başkaları tarafından ele geçirilmesi, dolandırıcılık, bilgisayar sistemlerine ve hizmetlerine hasar verme, kişisel ve önemli bilgilerinin kullanıcının haberi olmadan elde edilmesi gibi tehlikelerle karşı karşıyadır.

Bilgi ve Bilgisayar Güvenliği: CASUS YAZILIMLAR ve KORUNMA YÖNTEMLERİ kitabı, bilgi ve bilgisayar güvenliği konusunu, geniş bir perspektiften, tarihi gelişimi de göz ardı etmeyerek, her düzeyden bilgisayar kullanıcısının ilgisini çekecek şekilde gözler önüne sermektedir. Özellikle kişisel gizlik ve bilgi güvenliği konusunda, konu ile ilişkili tüm olgular, somut örnek ve faydalı tedbir önerileri ile ele alınmıştır.

Son zamanlarda bilgi ve bilgisayar güvenliği konusunda en ciddi tehditlerin başında yer alan kötücül yazılım (malware, "malicious software"), bulaştığı bir bilgisayar sisteminde veya ağ üzerindeki diğer makinelerde zarara yol açmak veya çalışmalarını aksatmak amacıyla hazırlanmış kötü niyetli yazılımların genel adıdır. Bilgisayar virüsleri, bilgisayar solucanları, Truva atları, arka kapılar, mesaj sağanakları (spam), kök kullanıcı takımları, telefon çeviriciler, korunmasızlık sömürücüleri, klavye dinleme sistemleri, tarayıcı soyma ve casus yazılımlar (spyware) en genel kötücül yazılımlardır.

Bilgi ve bilgisayar güvenliği literatüründe bir ilk olarak, ana kötücül ve casus yazılım türleri dışında; şu an için bilinen veya saptanabilen ve çok değişik amaçlara yönelik, akla gelmeyecek teknikler kullanan kırk kadar kötücül yazılım türü, temel özellikleri ile bir araya getirilerek açıklanmıştır.

## İÇERİK

Kitap, siz okuyucuların bilgi ve bilgisayar güvenliğine daha geniş bir çerçeveden bakabilmesini sağlamak amacıyla; genelden özele doğru bir anlatım mantığı ile hazırlanmıştır. Bu mantık içerisinde okuyucunun ilgisini ve bilgisini arttırmak için mümkün olduğunca güncel bilgilere yer verilmiştir. Kitabımızda sunulan bölümlerin içeriği aşağıda sırasıyla kısaca tanıtılmıştır.

**Kitabın Birinci bölümünde**, genel olarak bilgi ve bilgi varlıkları tanıtılmış ve değerlendirilmiştir. Çalışmanın özünü teşkil eden bilgi ve bilgi güvenliği konusu, en genel hatları ile incelenmektedir. Veri ve bilgi gibi, birbirleri ile karıştırılan ve birbirleri yerine söylenen terimler, açıklanmış ve bundan daha "rafine" anlam ve önem ifade eden "özbilgi" kavramı açıklanmıştır. Gerçeklik ile hikmet arasında yer alan veri, bilgi ve özbilgi basamakları, konuya farklı bir bakış açısı sunmak ve bilgi ve bilgi güvenliğinin temelini okuyucuya aksettirmek amacıyla sunulmuştur. Bu bölüm ile bilginin önemi ve değerinin daha da iyi kavranması ve bilginin korunması ve

güvenliğinin sağlanmasının işaret edilmesi amaçlanmaktadır.

**Bölüm 2**'de "Bilgi Güvenliği Tarihçesi" gözden geçirilmiştir. Bölüm, konunun zengin ve özgün bir çerçevede ele alınmasıyla bu alanda var olan boşluğu doldurmaya katkıda bulunacağı değerlendirilmektedir. Bu bölümde; şifre bilimi ve şifreleme teknikleri, kriptoanaliz senaryoları ve saldırılar ele alınmıştır. Şifrelemenin en eski örneklerinden Rosetta tableti, steganografi, anlamsız şifre, antik scytale ve Sezar şifreleri açıklanmıştır. Şifrelemenin din, mistik ve kültürel alanlarda çok ilginç kullanımları da bu bölü mde bir araya getirilmiştir. Hindistan'da Kama Sutra, semavi dinlerin ortaya çıktığı bölgede İbrani atbash şifresi, Kabala ve Tevrat içinde şifre inancı, Şeytanın Sayısı 666 muamması, hür masonların kullandığı domuz ağılı şifresi bu tip etkileşmelere örnek olarak aktarılmıştır. Müslüman bilim adamlarından modern şifreleme bilimine Frekans analizi ile kriptoanaliz yöntemi ile en büyük katkıyı sağlayan El-Kindi'nin anlatıldığı bu bölümde Ebcet hesabının Müslüman toplumlara etkisine de örnekler verilmiştir. Çok karakterli şifreleme, açık anahtar şifreleme, RSA açık anahtar algoritması, DES, özetleme algoritmaları ve PGP gibi günümüz şifreleme yaklaşımları ele alınmıştır. Bu bölümde, ayrıca ülkemizde şifreleme tarihi, Osmanlı ve Türkiye'de şifreleme ve ülkemizde modern kriptografi gözden geçirilmiştir. Bölüm genel olarak da ayrıca değerlendirilmiştir.

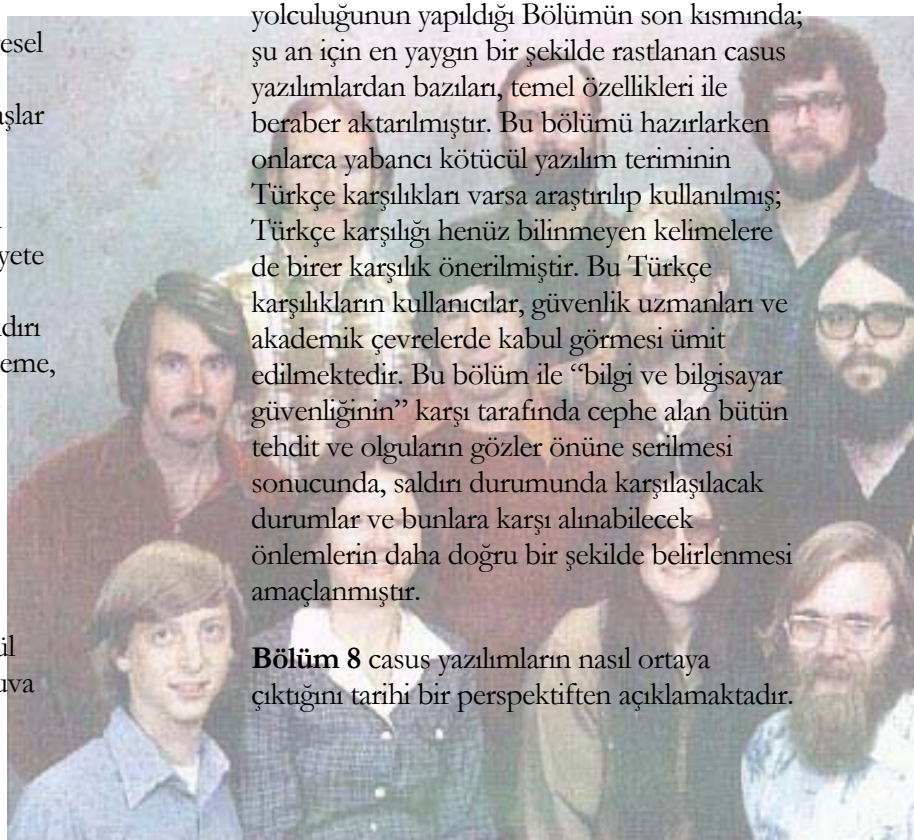
**Bölüm 3**'de genel olarak bilgi ve bilgisayar sistemleri güvenliği, önemi, ihtiyaç duyulan alanlar ve karşılaşılabilecek güvenlik açıkları gözden geçirilmiştir.

**Bölüm 4**'de, bilgi ve bilgisayar güvenliği ve güvenli bir sistemin taşıdığı bütün unsurlar açıklanmıştır. Sistematik bilgi güvenliği sürecinin en temel safhaları olan önleme, saptama ve karşılık verme süreçleri ve güvenlik risk yönetimi genel hatları ile bu bölümde özetlenmektedir.

Bilgi ve bilgisayar güvenliğinin günümüze kadar gelişimini kavramak adına sanal âlemin gelişimi ve "hacker" olarak adlandırılan bilişim korsanları **5. Bölüm**'de incelenmiştir. Bu bölümde siber uzay, bilişim korsanlığı ve korsanlık kültürü, sanal âlemin gerçek kişilikleri olan beyaz ve siyah şapkalı korsanlar, sistem kırıcılar, betik ve tıklama kerataları ve web sitesi tahrifatçıları ele alınmıştır. Gerek küresel ve gerekse yerel anlamda etkileri olan, korsanlık hareketi, siber terör ve siber savaşlar gözden geçirilmiştir.

**Bölüm 6**'da bilgisayar sistemlerine yapılan saldırıların yapıları ve türleri, güvenliği zafiyete düşüren saldırıların çeşitli şekillerde sınıflandırılması sunulmuştur. En genel saldırı türleri olan, kaynak kod istismarı, gizli dinleme, sosyal mühendislik ve insan hatası, hizmet aksattırma saldırıları, dolaylı saldırılar, arka kapılar, doğrudan erişim saldırıları ve kriptografik saldırılar bu bölümde açıklanmıştır.

**Bölüm 7**'de kötücül yazılımlar gözden geçirilmiş ve sınıflandırılmıştır. Ana kötücül yazılım türleri olan virüsler, solucanlar, Truva atları, casus yazılımlar, arka kapılar, mesaj sağanakları (spam), klavye dinleme sistemleri (keylogger), tarayıcı soyma, kök kullanıcı takımları (rootkit), telefon çeviriciler, casus yazılımlar ve korunmasızlık sömürücüleri özetlenmiştir. Ayrıca bu bölümde kırk kadar diğer kötücül yazılım türü gözden geçirilmiştir. Uzun araştırmalar sonucu elde edilen böyle bir sınıflamanın, ülkemizde yapılması beklenen araştırmalara bir temel oluşturacağı düşünülmektedir. Bu bölümde ayrıca; virüs, casus yazılım, mesaj sağanağı (spam), bilgisayar solucanı (worm), Truva atı (Trojan), reklâm yazılım (adware) ve sazan avlama (phishing) gibi kötücül yazılımların bir birleri ile olan ilişkisinden ve bilgisayar sistemlerine karşı sergiledikleri "bir nevi dayanışmadan" bahsedilmiştir. Casus yazılımların nasıl geliştiğine dair geçmişten günümüze bir zaman yolculuğunun yapıldığı Bölümün son kısmında; şu an için en yaygın bir şekilde rastlanan casus yazılımlardan bazıları, temel özellikleri ile beraber aktarılmıştır. Bu bölümü hazırlarken onlarca yabancı kötücül yazılım teriminin Türkçe karşılıkları varsa araştırılıp kullanılmış; Türkçe karşılığı henüz bilinmeyen kelimelere de birer karşılık önerilmiştir. Bu Türkçe karşılıkların kullanıcılar, güvenlik uzmanları ve akademik çevrelerde kabul görmesi ümit edilmektedir. Bu bölüm ile "bilgi ve bilgisayar güvenliğinin" karşı tarafında cephe alan bütün tehdit ve olguların gözler önüne serilmesi sonucunda, saldırı durumunda karşılaşılacak durumlar ve bunlara karşı alınabilecek önlemlerin daha doğru bir şekilde belirlenmesi amaçlanmıştır.



**Bölüm 8** casus yazılımların nasıl ortaya çıktığını tarihi bir perspektiften açıklamaktadır.

**Bölüm 9**'da yaygın casus yazılımlara örnekler verilmiştir.

**Bölüm 10**'da oldukça özgün ve bir o kadar da tehlikeli Klavye Dinleme Sistemleri bütün ayrıntıları ile tanıtılmıştır. Klavyeler ve çalışma prensipleri, klavye dinleme sistemi türleri olan donanım ve yazılım klavye dinleme sistemleri tanıtılmıştır. Ayrıca bu bölümde yazılım klavye dinleme sistemlerinin kullandıkları mekanizmalar ve işleyiş esasları ve mevcut klavye dinleme sistemleri açıklanmıştır. Klavye dinleme önleme sistemleri yine bu bölümde incelenmiştir. Klavye dinleme tabanlı yapıların bilgisayarlarda varlığını işaret eden bulgular, bu sistemlere yönelik alınabilecek tedbirler, güvenli bilgi girişi nasıl sağlanır ve İnternet üzerinde iz bırakmadan anonim gezinti nasıl yapılabilir gibi hususlar, ilgili başlıklar altında bu bölümde değerlendirilmiştir. Yazılım klavye dinleme sistemlerinin Windows işletim sistemine yönelik sergilediği, üç ana "ortadaki adam" (man-in-the-middle) saldırısının ayrıntıları ile incelenmiştir. Özellikle, Windows çengelleri (hook) konusunda oldukça önemli ayrıntılar sunulmaktadır. Çekirdek tabanlı klavye süzgeç sürücülü klavye dinleme sisteminin alt yapısının anlatıldığı bu bölümde, ayrıca Linux/BSD/UNIX benzeri işletim sistemlerinde klavye dinlemenin nasıl yapıldığı, örnek kod ile açıklanmaktadır. Klavye dinleme sistemlerinin sahip oldukları işleyiş esasları ve sahip olabilecekleri yetenekler sıralanmış; casusluk, ebeveynlerin çocuklarının İnternet (Genel ağ) ve bilgisayar kullanımını kontrolü ve işyeri gözetleme gibi birçok sahada klavye dinleme sistemlerinin nasıl kullanılabileceği ayrıntıları ile anlatılmıştır.

**Bölüm 11**'de Klavye dinleme sistemlerini önleyici yapılar ve yaklaşımlardan bahsedilmektedir.

**Bölüm 12**'de güncel kötücül ve casus yazılım vakalarına örnekler verilerek konunun vahameti ortaya konulmaya çalışılmıştır. Bu bölümde yurt dışında gerçekleşen olayların yanı sıra ülkemizde de son zamanlarda artış gösteren ve ön plana çıkan bilişim suçlarının en önemlileri ele alınmıştır. Böylelikle ülkemizin bu tür tehlikelere sanıldığı gibi uzak olmadığı hatta gün geçtikçe artan bir risk içinde olduğumuz gözler önüne serilmektedir.

SOYGUN

İki bilgisayar korsanının da yer aldığı çete, internetten gönderdikleri virüs sayesinde banka hesaplarına ulaştıkları şirketleri 3 trilyon lira dolandırdı. Banka görevlileri hesaplarından yüklü para çekilen şirketleri kontrol için aradığında telefona yine çete üyeleri çıktı. Çünkü bilgisayarla şirket telefonlarını kendi numaralarına yönlendirmişlerdi

**11 kişilik çete çökertildi**

Diyarbakır'da bir mermer şirketinin sahibi Beşir Yılmaz'ın polise "Şirket hesabından bilgim dışında 800 milyar çekildi" demesi üzerine başlıne dek hemen görülmemiş bir dolandırıcılık tezgahı ortaya çıkarıldı. Polis İstanbul ve Eskişehir'de eş zamanlı düzenlenen operasyonlarla aralarında 3 bilgisayar korsanının da (hacker) olduğu 11 kişilik dolandırıcılık çetesini çökertmeyi başardı.

**10 bin şirketin hesabı vardı**

Çetenin çeşitli şirketleri 3 trilyon lira dolandırdığı tespit edildi. Çete lideri Osman Özdek'in sevgilisi Sibel'in 17 yaşındaki banka hesabında 300 milyar lira bulundu. Çete üyelerinin dolandırdıkları parayla aldıkları BMW X5 ve BMW 320 otomobillere el konuldu. Çete toplam 10 bin şirket hesabına ulaşmıştı. Bu hesaplardaki para yaklaşık 40 trilyonu buluyordu. Yakalanmasalardı yarısı kendi hesaplarına aktaracaklardı.



İşte "Şifre" operasyonuyla çökertilen çetenin 4 üyesi.

**Ünlü bilgisayar korsanı**

İstanbul Emniyet Müdürü Celalettin Cerrah çetenin nasıl çalıştığını şöyle anlattı: İnternette 'Kilicbaigi' rumuzunu kullanan ve dünyanın sayılı bilgisayar korsanlarından biri olan Koray K. ile Fizik Mühendisi Samet B., şirketlere virüs alma bahanesiyle virüslü e-mail yolluyor. E-mail açıldığında şirket bilgisayarındaki banka hesaplarına ait bilgiler anında çetenin eline geçiyor.

**Sahte kimlikle çekiyorlar**

Şirket hesaplarındaki paralar internet bankacılığı kullanılarak çetenin açtığı hesapları aktarılıyor. Daha sonra adına hesap açılmış sahte kimlikli çete üyeleri gidip parayı çekiyor. Yüklü miktardaki para transferinden kuşkulanan banka görevlileri şirketi aradığında karşısına yine çeteden biri çıkıyor. Çünkü çete, bilgisayarla yönetilen şirket santralini de kendilerine ait telefona yönlendirebiliyor.

**Bölüm 13**'de bir bilgisayarda casus yazılımın var olduğuna işaret eden bulgular sunularak kullanıcıların tehlikelere karşı uyanık olmasına çalışılmıştır.

**Bölüm 14**'de casus yazılımların sistemlere bulaşma teknikleri, casus yazılımların "müşteri" ya da kurban çekme teknikleri, uç kullanıcı lisans antlaşması, kaçak indirme, program kaldırma mekanizması anlatılmaktadır.

**Bölüm 15**'de casus yazılımlara karşı alınabilecek önlemler aktarılmıştır. Bu bölümde sunulan ve aslında hiçte zor olmayan bu tedbirler ile kullanıcıların bilgi ve bilgisayar güvenlik seviyelerini çok yüksek seviyede tutulması mümkündür. Pek çok kullanıcı yeni bir bilgisayar satın aldığında hiç beklemeden bu bilgisayarı ile İnternet'e bağlanmaktadır. Hâlbuki bu çok önemli bir hatadır. İşte bu bölümde ayrıca birçok kullanıcının düştüğü bu hata ele alınmış ve bu hataya düşmemek için yapılması gerekenler sıralanmıştır. Yine bu bölümde herhangi bir bilgisayar programını satın alırken, bilgisayara kurmadan önce ve kullanırken dikkat edilmesi gereken hususlar da ele alınmıştır.

**Bölüm 16**'da casus yazılımların otomatik başlatma yöntemleri aktarılmıştır. Birçok kötücül ya da casus yazılım bu yöntemleri kullanarak bulaştıkları sistemlerde ikamet edebilmektedirler. Bu yöntemleri bilmek bu tür kötü niyetli yazılımları saptayabilmeniz açısından oldukça faydalı olabilir.

**Bölüm 17**'de bit sonlandırma yöntemi ile ActiveX engelleme, İnternet gezginini ağ kullanıcıları için yapılandırma, casus yazılım bulunan konak (host) sunucuların önlenmesi, virüs koruma programları ile casus yazılım koruyucular bu bölümde ayrıntılı bir biçimde açıklanmıştır.

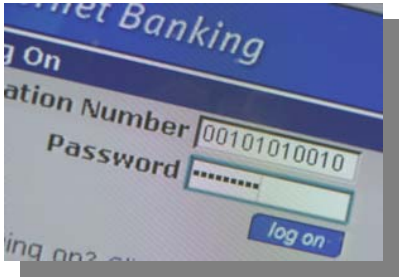
**Bölüm 18**'de casus savar yazılımları ve Microsoft Windows işletim sisteminde

kullanılabilecek diğer güvenlik araç ve yazılımları tanıtılmıştır.

**Bölüm 19**'da Microsoft'un 2007 yılının başında çıkartmayı planladığı yeni işletim sistemi Microsoft Windows Vista'nın ve bu işletim sistemi ile tanıtılacak Windows İnternet Explorer Tarayıcı 7'nin getirmiş olduğu yeni güvenlik teknolojileri ve alt yapısı ayrıntıları ile tanıtılmıştır.

**Bölüm 20**'de ise günümüzde bilgisayar kullanımında en hevesli ve becerikli kesimlerden biri olan çocuklarımızı, karşılaşabilecekleri tehditlerden korumak ve aileleri bu konuda uyarmak için, bilinmesi ve uygulanması gereken önemli birçok husus farklı başlıklar altında açıklanmıştır.

**Bölüm 21**'de işyeri ve elektronik gözetleme konusu güvenlik ve casus yazılımlar açısından ele alınmıştır. Bu bölümde işyerlerine yönelik güvenlik açıkları, işyeri gözetleme ve sonuçta bundan faydalanabilme ve gerekli önlemlerin alınması konuları açıklanmıştır.




**Bölüm 22**'de ise kişisel gizlilik ve bilişim suçları ve bilişim suçlarına yönelik yasal düzenlemeler değerlendirilmiştir. Bilgi ve bilgi güvenliği konusunda önemli ve üzerinde gerçekleşen tartışmaların hala devam ettiği bir konu olan, kişisel gizlilik (mahremiyet), temel özellikleri ile beraber sunulmuştur. Bölümün sonunda ülkemizde yeni Türk Ceza Kanunu ile tanımlanan ve konu ile ilişkili olan "Bilişim Suçları" kanunları konunun yasal boyutunu da sergilemek amacıyla sunulmaktadır.

**Ek bölümlerde**, kitapta kullanılan terimlerin kısaltmalar, İngilizce ve Türkçe karşılıkları, ulusal ve uluslararası İnternet bölge kodları gibi faydalı olabilecek veriler sunulmaktadır.



## SONUÇ

Bu kitap baştan sona akademik bir anlayışla hazırlanmış, faydalanılan kaynaklara yerinde atıflar yapılmış ve her bölümü özgün çalışmalardan oluşmuştur. Konunun daha iyi anlaşılmasına yarar sağlayacak, çoğu özgün bir şekilde hazırlanmış olan zengin görsel içerik de kitap ile beraber sunulmuştur. Sadece ülkemizde değil; dünyada da bu konuda yazılmış böyle bir kapsamlı çalışmanın bulunmadığını da burada vurgulamak isteriz.

Bu kitabın ülkemizde İnternet kullanıcılarına, lise ve üniversite öğrencilerine, kişisel gizlilik ve fikri mülkiyet haklarını korumak ve bu konularda çalışma yapmak veya yaptırmak isteyenlere, işyeri sahiplerine ve çalışanlarına, çocuklarını İnternet'teki tehlikelerden korumak isteyen anne ve babalara, üniversite öğretim elemanlarına, güvenlik güçlerine, bu konuda kendini yetiştirmek isteyenlere ve hatta bu konuda uzman birçok bilgisayar kullanıcısına katkı sağlayacağı değerlendirilmektedir.

## KİTAP SİPARİŞ/İSTEK

Bilgi ve Bilgisayar Güvenliği: CASUS YAZILIMLAR VE KORUNMA YÖNTEMLERİ kitabını edinmek isterseniz, kitap@canbek.com e-posta adresi ile irtibata geçiniz.

## DAHA FAZLA BİLGİ

Bilgi ve bilgisayar güvenliğine önem vermemenin, size, çocuklarınıza, işyerinize ve ülkemize maliyeti, zannettiğinizden çok daha fazladır. O halde neden hemen şimdi bu konuda yapabileceklerinizi öğrenmek istemiyorsunuz?

http://www.canbek.com/BBG