



*BİLGİ İŞLEM DAİRE BAŞKANLIĞI*

# ISO 27001: BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

FARKINDALIK EĞİTİMİ

25.02.2019

Bursa Teknik Üniversitesi  
Bilgisayar Mühendisliği Bölümü  
Ahmet Kaşif - Gizem Ortaç

# AJANDA

- Temel Kavramlar
- Bilgi GüvenliĐinin Önemi
- Ülkemizde Bilgi GüvenliĐi
- Tehditler
- Hack ve Hacker Kavramları
- Saldırı Türleri
- Yasal Sorumluluklar
- Bilgi GüvenliĐi Politikaları
- Roller ve Sorumluluklar

# Temel Kavramlar

**Bilgi güçtür.**

Francis Bacon (1561-1626)

# Temel Kavramlar

- **Bilgi Güvenliđi:** Bilginin, bilgi güvenliđi ölçütlerinin etkin kullanımı ile korunmasını hedefler. Kađıt bir evrak, insan hafızası, telefon konuşmaları gibi bilgiler, bilgi güvenliđi kapsamında değerlendirilir.
- **Siber Güvenlik:** Elektronik ortamda üretilen, iletişim halinde olan ve saklanan bilginin güvenliđi, siber güvenlik kapsamında değerlendirilir.

# Temel Kavramlar

- Bilgi Güvenliđi Ölçütleri
  - Gizlilik: Bilgi sadece erişim ve kullanım yetkisi bulunan taraflarca değerlendirilebilmelidir. Harici tüm taraflara karşı koruma sağlanmalıdır.
  - Bütünlük: Bilgi deđişime ve bozulmaya karşı korunmalıdır.
  - Erişilebilirlik: Bilgi ulaşılabilir olmalıdır.

# Bilgi Gvenliđinin nemi

- Bilgi gvenliđinin sađlanamadıđı durumlarda,
  - Kiři veya kurumlara ait gizli ve hassas bilgiler ađıđa ıkabilir.
  - Bilgiye eriřim mmkn olmayabilir.
  - Bilgi ieriđi yetkisiz kiřiler tarafından deđiřtirilebilir.
  - İř srekliliđi zarar grebilir veya aksayabilir.
  - Ticari, teknolojik ve adli zararlar meydana gelebilir.

# Ülkemizde Bilgi Güvenliđi

- Siber Güvenlik Eylem Planı : Ülkemizde Siber Güvenlik alanında ilk eylem planına yönelik ilk alıřma 2012 yılı Aralık ayında gerekleřtirilmiřtir.
- BTK (Bilgi Teknolojileri Kurumu): Telekomünikasyon sektörünün düzenleyici kurumu olarak görev yapmaktadır ve yetkilendirme, denetleme, ihtilaf özümü, tüketici haklarının korunması, sektör rekabetinin düzenlenmesi, teknik yönergeler yayınlamak ve spektrum yönetimi ve izlenmesinden sorumludur.

# Ülkemizde Bilgi Güvenliđi

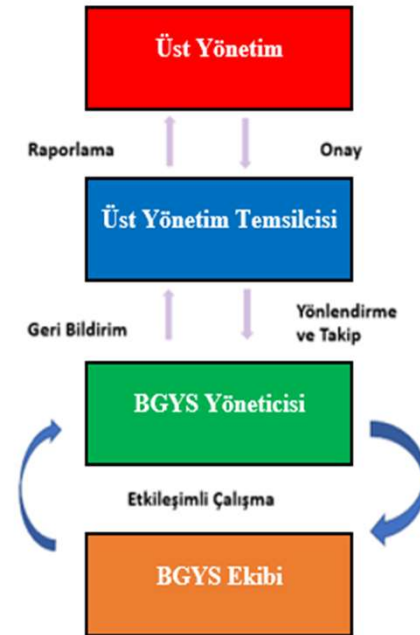
- Bursa Teknik Üniversitesi de Siber Güvenlik Eylem Planı kapsamında BGYS teşkilatını kurmuştur. Bu yapının amaçları şunlardır;
  - Tüm bilgi varlıklarının güvenliđinin sağlanması,
  - Erişim kontrol politikası oluşturulması,
  - Parola politikası Belirlenmesi
  - Kurum içi geliştirilen yazılımların güvenliđinin sağlanması
  - Mobil cihaz kullanım politikası oluşturulması
  - Bilgi akışı politikasının oluşturulması
  - Sürekli iyileştirme için gerekli yönetimin oluşturulması



# Ülkemizde Bilgi Güvenliđi

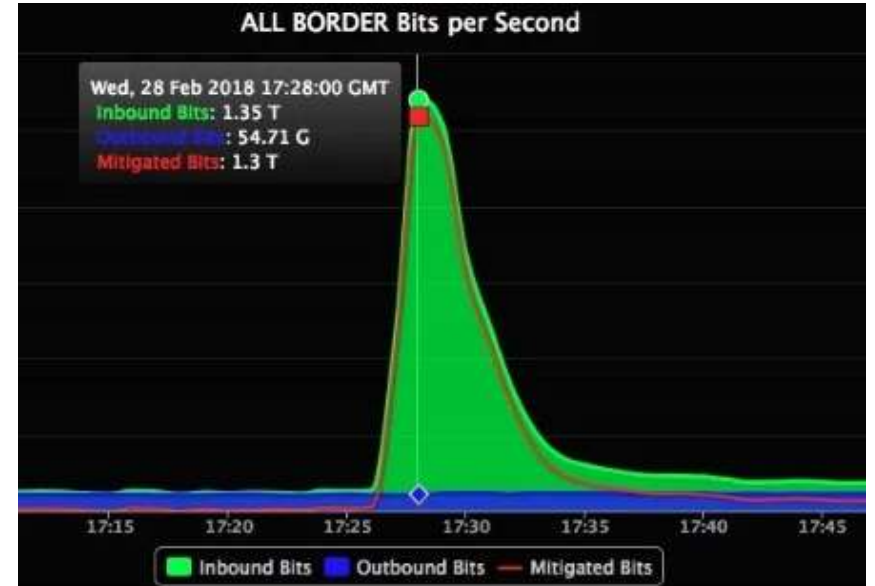
- 5651, 5070 ve 5846 Sayılı Kanunlar
- TCK Madde 135 (Kişisel verilerin kaydedilmesi)
- TCK Madde 136 (Verileri hukuka aykırı olarak verme veya ele geçirme)
- TCK Madde 243 (Bilişim sistemine grime)
- TCK Madde 244 (Sistemi engelleme, bozma, verileri yok etme veya deđiştirme)
- TCK Madde 326 (Devletin güvenliğine ilişkin belgeler)
- TCK Madde 327 (Devletin güvenliğine ilişkin bilgileri temin etme)
- TCK Madde 328 (Siyasal veya askeri casusluk)
- TCK Madde 329 (Devletin güvenliğine ve siyasal yararlarına ilişkin bilgileri açıklama)
- TCK Madde 330 (Gizli kalması gereken bilgileri açıklama)
- SPK Bilgi, Belge Ve Açıklamaların Elektronik Ortamda İmzalanarak Kamuyu Aydınlatma Platformuna Gönderilmesine İlişkin Esaslar Hakkında Tebliđ

# BGYS Sorumlulukları



# Güncel Saldırılar

- 2016 yılında GitHub'a 1.35 Terrabit/saniye büyüklüğünde DDoS saldırısı gerçekleştirildi.
- Saldırı 15-20 dakika sürdü, bu sırada dünyanın çeşitli yerlerinde erişim sıkıntısı oluştu.
- Bilgi güvenliği politikasını doğru oluşturduğu ve zamanında müdahale edildiği için, GitHub bu saldırıdan büyük bir başarıyla kurtuldu.



# Güncel Saldırılar



# Hack ve Hacker

- Hack: Bir materyal, araç, cihaz ya da nesnenin amacı dışında kullanılmasıdır.
- Hacker: Belirli bir sorunu çözmek için yeterli teknik bilgiye sahip uzman bilgisayar kullanıcısıdır. Yaygın kullanılan tanımı ise güvenlik açıklarını kullanarak sistemlere sızan kişilerdir.
  - Beyaz şapkalı hacker: Bilgi güvenliğini sağlama amacıyla siyah şapkalı hacker'lara karşı savunma ve saldırı faaliyetlerini yürüten kişilerdir.
  - Siyah şapkalı hacker: Belirli bir sistem, araç veya bilgiye yönelik erişim, bozma ve ele geçirme gibi kötü niyetli amaçlar doğrultusunda çalışan uzman bilgisayar kullanıcılarıdır.

# Siber Saldırı Süreçleri

- Hedef hakkında bilgi toplanır.
  - Bilgi paylaşımı yaparken daha seçici olunmalıdır.
- Hedefin zayıf noktaları belirlenir ve en uygun saldırı yöntemine karar verilir.
  - Zayıf noktalarımızı belirlemeli, korumak için önlem almalıyız.
- Belirlenen yöntem uygulamaya geçirilir.

Hiçbir sistem tam güvenliği garanti etmez, amaç saldırganın işini zorlaştırmak olmalıdır.

# Saldırı Türleri

- Parola Güvenliği: Elektronik ortamlarda kullanılan parolalar elektronik bilginin korunmasında ve izinsiz erişimin önlenmesinde kullanılmaktadır.
- Parolamızı belirlerken dikkat edilmesi gereken hususlar şunlardır:
  - 12 karakterden oluşmalıdır.
  - Rakam, harf ve özel işaretlerin kombinasyonundan oluşmalıdır. Her birinden en az birer tane içermelidir. Büyük küçük harf kullanılabilir.
  - Kişisel bilgilerimizi kısmen ya da tamamen, doğrudan ya da dolaylı (tersten yazma, iki bilgiyi bölerek birleştirme, belirli harflerini kullanma vs.) olarak içermemelidir.
  - Her ortamda farklı şifre kullanılmalıdır.


# Amount of Time to Crack Passwords

"abcdefg" 7 characters  .29 milliseconds

"abcdefgh" 8 characters  5 hours

"abcdefghi" 9 characters  5 days

"abcdefghij" 10 characters  4 months

"abcdefghijkl" 11 characters  1 decade

"abcdefghijkl" 12 characters  2 centuries



# Character Type Difference

Combining ASCII, Lowercase, Uppercase, and Numeric

**"Password"**

Cracked just under the time  
it would take lightning to strike 2-3 times

**"P@sswOrD"**

Will be cracked in the same amount of time  
it took to carve Mt. Rushmore, or 14 years.

# Passwords Weaken Over Time

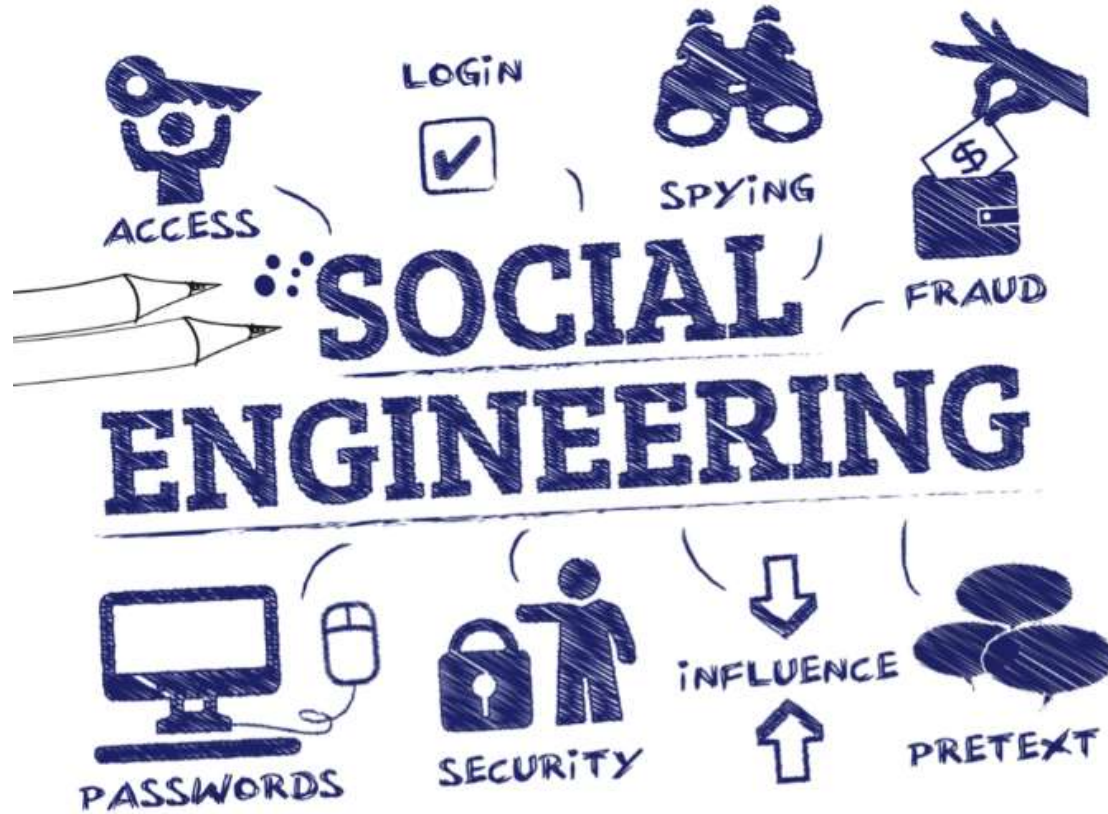
Discover How a Password Becomes Less Secure Through the Years

Time It Takes to Crack the Password:

**security1**

<b>2000</b> Year	<b>3</b> Years	<b>10</b> Months	<b>1</b> Week	<b>5</b> Days	<b>14</b> Hours	<b>54</b> Minutes	<b>19</b> Seconds	<b>29</b> Seconds	<b>1.37</b> Milliseconds
<b>2001</b> Year	<b>2</b> Years	<b>9</b> Months	<b>0</b> Week	<b>5</b> Days	<b>11</b> Hours	<b>28</b> Minutes	<b>35</b> Seconds	<b>4</b> Seconds	<b>10</b> Milliseconds
<b>2002</b> Year	<b>2</b> Years	<b>1</b> Months	<b>3</b> Week	<b>0</b> Days	<b>22</b> Hours	<b>20</b> Minutes	<b>41</b> Seconds	<b>9</b> Seconds	<b>4</b> Milliseconds
<b>2003</b> Year	<b>1</b> Year	<b>9</b> Months	<b>1</b> Week	<b>6</b> Days	<b>18</b> Hours	<b>22</b> Minutes	<b>50</b> Seconds	<b>32</b> Seconds	<b>6</b> Milliseconds
<b>2004</b> Year	<b>1</b> Year	<b>0</b> Months	<b>1</b> Week	<b>2</b> Days	<b>1</b> Hours	<b>57</b> Minutes	<b>49</b> Seconds	<b>50</b> Seconds	<b>6</b> Milliseconds
<b>2005</b> Year	<b>0</b> Years	<b>7</b> Months	<b>1</b> Week	<b>5</b> Days	<b>6</b> Hours	<b>6</b> Minutes	<b>52</b> Seconds	<b>12</b> Seconds	<b>5</b> Milliseconds

# Saldırı Türleri - Sosyal Mühendislik



# Sosyal Mühendislik

- Bir sosyal mühendisin temel özelliği, **basit** fakat genelde amacına ulaşan **donanımlar** ve **teknikler** kullanarak saldırı yapmasıdır.
- Sosyal Mühendislik (Social Engineering), internet korsanlarının hedeflerinde yer alan kişiyi aldatarak, istediği bilgileri ele geçirmesini sağlayan bir saldırı tekniğidir. Diğer siber korsanlık terimlerinin aksine sosyal mühendislik teknik olmayan bir terimdir.
- Sosyal mühendislerden sahip oldukları bu yetenekleri ve teknikleri iyi yönde kullananlar **beyaz şapkalılar**; kötü niyetle kullanmak isteyenler ise **siyah şapkalılar** olarak adlandırılır.

# Sosyal Mühendislik

Sosyal Mühendislerde bulunması gereken özellikler aşağıdaki gibidir :

- İkna etme yetenekleri gelişmiştir.
- Etkileme özelliği yüksektir.
- Aldatmaktan çekinmezler her yolu mübah görürler
- Bilgili ve donanımlı olduğunu karşı tarafa gösterme
- Senaryo üretme yetileri oldukça fazladır.

Sosyal mühendislikte en sık kullanılan yöntemlerden biriside Phishing yani oltalama birazda ondan bahsedelim.

## Phishing Nedir ?



Türkçe karşılığı oltalama olan **Phishing**, İnternet kullanıcılarının kredi kartı ve banka hesap numaraları ve bu hesaplara ait şifre ve CVV2 numaraları gibi hassas içerikleri elde etme amacıyla saldırgan tarafından yapılan sosyal mühendislik saldırılarından biridir. Bu saldırılarda kandırılan kullanıcı, oltaya takılan bir balığa benzetildiği için “oltalama” adını almıştır.

# Phishing Saldırısı Nasıl Yapılır?

- Phishing saldırılarında kullanıcı genelde sahte bir e-posta vasıtasıyla tuzağa düşürülür. Saldırıcıyı yapan kötü niyetli kişi, doğrudan temas yeri bilinen ve güvenilen banka ,firmaları kullanarak hedeflenen bilgilere ulaşmayı sağlar.

## ***Genel saldırı senaryosu :***

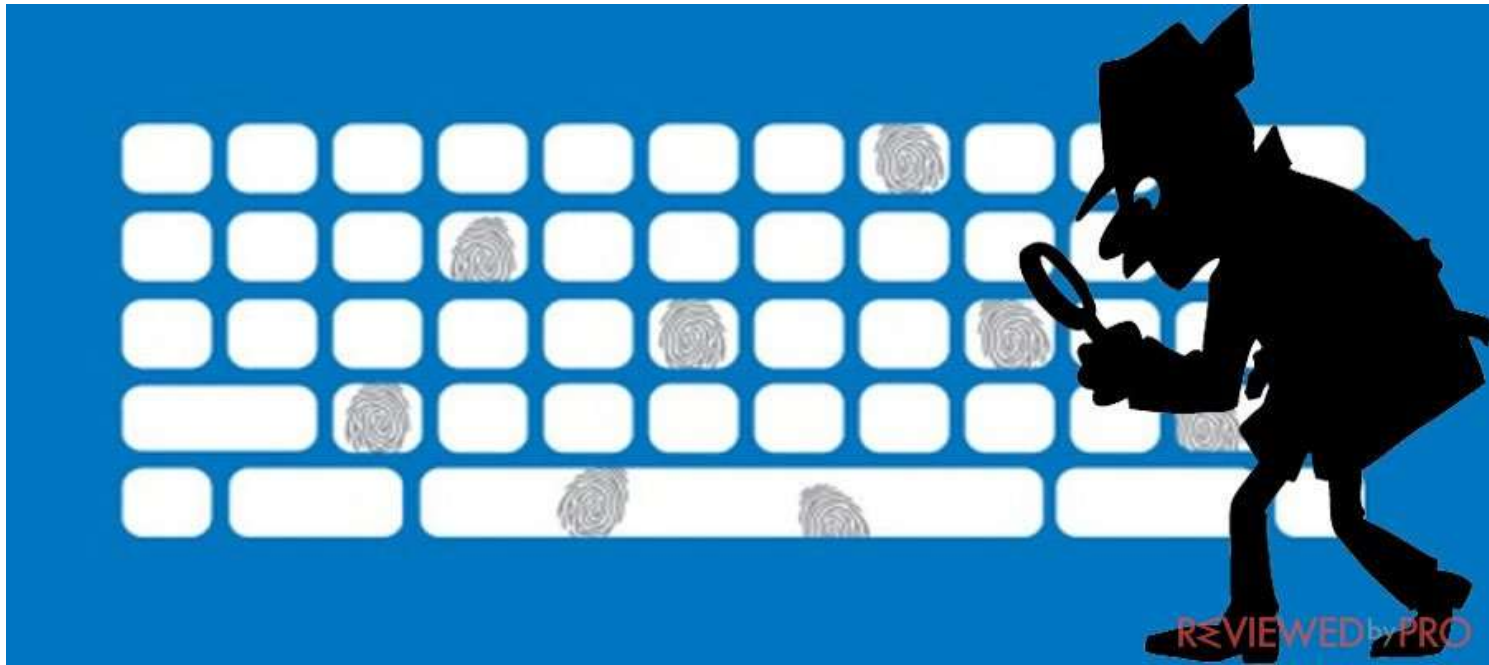
- Kötü niyetli kişi, genelde bankaların kimliklerini kullanarak hedef kullanıcıya bir mail gönderir. Gönderilen mailin içeriğinde sistemde yapılan güncellemeler veya yenilikler nedeniyle kullanıcının verilen adrese bilgilerini girmesi gerektiği söylenir. Mail aracılığı ile iletilen adres kimliği kullanılan kurumun birebir kopyasıdır. Oltalanan kişi bu siteyi gerçek site sanarak girip bilgilerini yazınca tüm bilgiler artık kötü niyetli kişinin eline geçmiş olur.

# Peki bu saldırıdan nasıl korunabiliriz ?

- **Güvenilir kaynaklar bilgi istemez** : Müşterisi olduğunuz kurumların sizlerin bilgilerine ihtiyacı yoktur. Mail ya da siteler aracılığıyla kullanıcı adı ve parolalarınızı talep eden bağlantıları önemsemeyiniz.
- **Tanımadığınız mailleri açıp okumayın** : Tanımadığınız kişi veya kurumlar tarafından yollanan mailleri okumadan direkt siliniz. Bu tür mailler sizleri Phishing saldırısı ile oltalayabilir. Aman dikkat :)
- **Adres kontrolü yapınız** : Phishing saldırılarında oltaya takılmamanın en önemli unsurlarından biride tarayıcıda bulunan adresi kontrol etmektir. Bir karakter değişikliği umulmadık sonuçlara yol açabilir.
- **Güvenlik Kontrolü yapınız** : Bankalar, alışveriş siteleri gibi kullanıcı bilgileri ve havale işlemlerinde **HTTPS** güvenli protokolü kullanılır. Bu protokolde yapılan veri iletimi şifrelenerek yapılır ve güvenlik üst düzeydir.
- **Hesap özetinizi kontrol ediniz** : Düzenli aralıklarla kontrol ediniz. Mail adresinize gönderilen e-postaları silmeyin ve adresin yönlendirildiği site hakkında, Whois veritabanlarından bilgiler toplayabilirsiniz. Bu bilgileri savcılığa göndererek şikayette bulunabilirsiniz.



# Saldırı Türleri - Keylogger



# Keylogger

- Keylogger basitçe sizin klavyeden yaptığınız her vuruşu kaydeden ve bu kayıtları kişisel bilgilerinizi çalmak isteyen kişilere gönderen programlardır. Bu kişiler istedikleri zaman bunlara ulaşıp yazdığınız her tür bilgiyi görebilirler. Bu yolla sizin e-mail şifreniz, kredi kartı numaranız gibi hayati önem taşıyan bilgileriniz çalınabilir.

# Keylogger

- Keylogger eğer sistem yöneticisinin bilgisi dahilinde yüklenmişse tamamen sistem güvenliği için çalışmaktadır.Fakat bu yazılım veya donanım sistem yöneticisinin bilgisi olmadan yüklenmişse tamamiyle saldırı ve casusluk amacı taşır.
- **Yazılımla Çalışan Keyloggerlar:** Sisteminize yüklenmesiyle aktif hale gelen tuş takip programlarıdır , klavyenizde basılan her tuşu bir dosyaya kaydeder.
- **Donanımla Çalışan Keyloggerlar:** Bilgisayarınıza bir donanım eklemesiyle aktif hale gelen tuş takip cihazıdır , klavyenizde basılan her tuşu bir kalıcı bellek kartına yazılıma ihtiyaç duymadan kaydeder. ( klavye ile anakart arasına takılan küçük , Dikkatli bakılmadan görülemeyecek aparatlardır)

# Keylogger

- **Güvenlik Amaçlı Keyloggerlar;** Genelde ebeveynlerin çocuklarını internet başındayken takip etmeleri için kullanılır ve tamamen sistem yöneticisinin bilgisi dahilindedir.

**Saldırı Amaçlı Keyloggerlar ;** Güvenliğinizi tehdit eden keyloggerlar çeşitli yollardan bilgisayarınıza bulaşabilir. Bu yollardan en yaygını herhangi bir programın içine keylogger yerleştirilerek sisteminizde çalıştırılmasıdır. Şüphesiz en büyük tehdit şüphesiz eş zamanlı mesajlaşma programları ( msn , icq , Yahoo , google talk v.b. ) Bir saldırgan size herhangi bir dosya gönderebilir saldırgan gönderdiği bu dosyanın içine (genelde program veya fotoğraf olur) keylogger yerleştirebilir. Gönderdiği dosya çalışıyor gözükürken aslında arka taraflarda bilginiz dahilinde birde keylogger çalışmaya başlamıştır.

- Bu andan itibaren saldırganın kendinizi teslim etmiş olursunuz en zor iş bitmiştir. Artık saldırganın yapacağı tek şey bilgisayarının başına geçip sizin klavyenizde bastığınız tuşları takip etmektir.

# Keylogger

- Keylogger sisteminize bulaştıktan sonra saldırganın konfigüre edişine göre Bastığınız tuşların kaydını içeren dosya ya saldırganın belirlediği e posta adresine gelir yada web sitesinde arşivleyebilir. Ayrıca saldırgan bastığınız tuşları anlık olarak takip edebilir ve istediği bilgiyi sizden alır almaz saldırı işlemlerine başlayabilir.

## **Keylogger Türü Yazılımlar Sisteme Nasıl Giriyor?**

- Kötü niyetli kişiler tarafından yazılan ve işletim sistemlerinin açıklarından yararlanılarak hedef bilgisayarın kısmen veya tamamen yönetici haklarını saldırgana teslim eden truva atı (trojan) adlı yazılımlar aracılığıyla keylogger yazılımları sisteme yüklenebilir.
- Keylogger yazılımı bilgisayara kullanıcı tarafından yüklenebilir.

# Keylogger

## **Keylogger ve benzeri programlardan etkilenmemek için:**

- Mutlaka işletim sisteminizin güncelleştirmelerini yapın.
- Bir güncel ve aktif antivirüs programını bilgisayarınızda bulundurun.
- Bankacılık ve önemli işlemlerinizi güvenli olmayan bilgisayarlardan yapmayın.
- Kullandığınız bilgisayarın web browserı (internet tarayıcısı)nın otomatik tanımlama özelliğindeki Formlarda kullanıcı adları ve parolalar ile ilgili kısmın işaretli olmasına dikkat edin.

# Mobil Cihazlarda Güvenlik

## VARSAYIMSAL RİSKLER TAKİP EDİLİYORUZ!

Mobil sistemlerin yaygınlaşması ve akıllı cep telefonlarının yoğun kullanımı, hackerların dikkatini bu yöne doğru çekiyor.

Akıllı telefonlar, klasik bilgisayar sistemleri ile yapılabilen her şeyi yapmak üzere geliştirildiği için riskler de o oranda artmıştır.

### iPhone ve iPad 3G Her Hareketinizi ve Her Çağrınızı Takip Ediyor

Nerede? Bu bir sır! 😊



**Apple'dan sevgilerle:** "Her Hareketinizi ve Çağrınızı İzliyoruz!" Tüm dünya bugün (20.04.11) California Santa Clara'da düzenlenen "Where 2.0" 2011 konferansında *Alasdair Allan* ve *Pete Warden* adlı araştırmacıların **iPhone** cep telefonunun ve **iPad 3G** mobil cihazının kullanıcıların her hareketini gizli bir dosyada kaydettiğini açıklamasıyla sarsıldı. Peki bu nasıl gerçekleşiyor ve Apple'ın derdi ne?



### iPhone ve iPad Verilerine Uzaktan Erişilebiliyor



**Elcomsoft Phone Password Breaker** isimli bir adli bilişim aracı, iPhone ve iPad'lerin tüm verilerine cihazla herhangi bir fiziki temasa girmeden gerçek zamanlı olarak erişilebiliyor. Böylelikle adli bilişim işlerini oldukça kolaylaştırıyor. Tabi bunun yanında eğer isterse bütün verilere her daim ulaşabiliyor. Araç, iPhone ve iPad'ini yedeklemek için **iCloud**'u kullanan ürün sahiplerini hedef alıyor.

# Mobil Cihazlarda Gvenlik

- Sahte aramalara dikkat!
- Kurulan yazılımların kullanmaları gereken kaynaktan fazlasına erişim istemesi
- Arka planda çalışan yazılım ve servislerin izlenmesi
- Gvenlik ayarlarında bilinmeyen kaynaktan yazılım yklenmesine engel olmak
- Mobil anti virs kullanmak periyodik tarama yapmak, gereksiz veya gvenilmeyen uygulamaları kaldırmak
- Mobil cihaz ynetim yazılımını kullanmak
- İşletim sistemini gncel tutmak
- Market zerinde uygulama yayıncısını dođrulamak

**Kurumsal bilgileri ve parolaları mobil sistemlerde Őifreli olarak tutulmalı!**





# Kablosuz Ağ Güvenliđi

- **Kafeler, restoranlar, hastaneler, havaalanları ve benzeri birçok yerde** kablosuz ađları kullanılmaktadır. Hatta işyerimiz ve evimizde bile artık mobil olmaya çalışıyor ve kablosuz olarak interneti kullanıyoruz.
- Siber saldırganlar güvensiz ađlara sızarak, ađ üzerindeki iletişiminizi dinleyebilir, sizi sahte sitelere yönlendirebilir veya kredi kartı gibi kritik bilgilerinizi çalabilirler. Bu noktada kablosuz ađımızı hem iş yerlerimizde hem de evimizde korumak zorundayız.
- **Diđer bir risk ise havaalanları, oteller, kafeler veya hastaneler gibi halka açık alanlarda güvenliđi sağlanmamış kablosuz ađlardır.**



# Kablosuz Ağ Güvenliğini Nasıl Sağlarım?

## 1. Kablosuz Ağınızın Adını Deęiřtirin

SSID olarak bilinen Wifi ağ adınızı deęiřtirmek güvenlik için ilk adım olacaktır. Genel olarak tüm modemler ve kablosuz ağ özelliğine sahip cihazlar varsayılan bir SSID ismi ile yayın yaparlar. Bu adı deęiřtirmeniz kötü niyetli siber saldırganlara karşı sizi güvende tutacaktır. Çünkü genel olarak varsayılan SSID isimlerine kablosuz cihazların adı ve model numaraları yer almaktadır. Unutmayın siber saldırganlar sizin veya kullandığınız teknolojiler hakkında ne kadar bilgi elde ederlerse o kadar başarılı saldırılar yapabilirler.

## 2. Kablosuz Ağınız İçin Güçlü Bir Parola Kullanın!

Parola kullanımı en önemli güvenlik unsurlarından biri olarak kabul edilir. Zayıf, tahmin edilebilir veya basit bir parola kullanırsanız, siber saldırganların işlerini kolaylařtırmış olur ve ağınızın çok çabuk ele geçirilmesine neden olabilirsiniz.

# Kablosuz Ağ Güvenliğini Nasıl Sağlarım?

## 3. Parolanızı Hiç Kimse İle Paylaşmayın!

En önemli kural ise parolanın hiç kimse ile paylaşılmamasıdır. Genelde evlerimizde kablosuz ağ kullanırken komşularımız bizden internet parolasını isteyebilir, arkadaşlarımız, misafirlerimiz dahi kısa süreliğine bile olsa sizden kablosuz ağ parolanızı isteyebilir. Bu da güvenlik için büyük bir risktir! Siz ne kadar güvende olursanız olun, komşunuz veya evinize gelen bir misafirin virüslü cihazı sayesinde kablosuz ağınızda siber saldırganlara özel bir kapı açmış olabilirsiniz.

## 4. Güçlü Bir Ağ Şifrelemesi Kullanın

Modem veya Hotspot ayarlarınızda **WEP, WPA, WPA2** gibi birçok şifreleme metodunu kullanabilirsiniz. WEP şifreleme metodu çok eski yıllarda geliştirilmiş günümüz şartlarına göre maalesef ki aşılması çok kolay hale gelmiş bir teknolojidir. Aynı şekilde WPA şifreleme metodu da yaygın olarak kullanılsa bile güvensiz şifreleme metotları arasında sıralanır. Tavsiyemiz ise modeminiz destekliyorsa WPA2 + AES kullanmanızdır. AES askeri şifreleme metotlarından biridir. Kablosuz ağınızı WPA2 + AES kullanımı ile güçlü bir hale getirebilirsiniz.

## 5. İşte ya da Evde Değilseniz ve Tatile Çıktıysanız Kablosuz Ağı Kapatın

Uzun süreli tatil dönemlerinde yani modeminizden uzak olduğunuz zamanlar modeminizi veya Hotspot (kablosuz ağ) desteğini kapatmak, korsanlara karşı büyük bir avantaj sağlayacaktır. Korsanlar genel olarak parola kırmak için brute force (deneme / yanılma) yöntemini kullanırlar. Bu noktada tatile çıkmanız onlar için büyük bir fırsat sağlar. Ancak kablosuz ağınızı tatile çıkarken kapatırsanız bir adım daha güvende olabileceğinizi rahatlıkla söyleyebiliriz.

# Kablosuz Ağ Güvenliğini Nasıl Sağlarım?

## 6. Uzaktan Yönetim Özelliğini Kapatın

Genel olarak modemler, routerlar veya hotspot hizmeti sunan cihazlar uzaktan yönetilebilir şekilde karşımıza gelirler. Uzaktan yönetimi kullanmıyorsanız, modem ayarlarınızdan bu özelliği kapatarak güvenliğinizi artırabilirsiniz. Uzaktan yönetim özelliği modeminize başka bir internet bağlantısı üzerinden yani farklı bir lokasyondan ulaşmanızı ve yönetebilmenizi sağlar. Güçlü parola kullanımında olduğu gibi modem yönetim şifrenizi de güçlü hale getirmenizi, bu özelliği kullanmadığınız takdirde kapatmanızı tavsiye ederiz.

## 7. Güncel Cihaz Yazılımları Kullanın

İşletim sisteminizi, kullanmış olduğunuz yazılımları ve güvenlik programlarını güncel tutmak güvenliğin sağlanmasındaki en önemli adımlardan biridir. Yazılımlarımızı güncel tutmamız gerektiği gibi kullanmış olduğumuz [Firewall](#), Router, [hotspot](#) ve modem gibi cihazların da güncel yazılımlar kullanması gereklidir.

## 8. Güvenlik Duvarı (Firewall) Kullanın

Güvenlik duvarları ([Firewall](#)) genel olarak birçok cihazın içerisinde gömülü olarak sunulmaktadır. Kablosuz ağ ([hotspot](#)) hizmeti sağlayan cihazların içerisinde de varsayılan olarak karşımıza gelmektedir. Ancak birçok kullanıcı modem ayarlarını yaparken Firewall özelliğini aktif etmez veya varsayılan olarak karşımıza kapalı gelebilir. Bu durumda elbette ki siber saldırganların ataklarına karşı korumasız bir hale geliriz.