DÜZCE
ÜNİVERSİTESİ

# Bilgi Güvenliği

Gölyaka MYO Bilgisayar Programcılığı

Güvenliğin sadece küçük bir bölümü teknik güvenlik önlemleri ile sağlanır.
Büyük bölümü ise kullanıcıya bağlı.

**Pareto prensibi: Önlemlerin %20'si -> saldırıların %80'inden korur.**

# İÇERİK

- Temel kavramlar
- Bilgi güvenliği neden önemli?
- Bilgi güvenliğine yönelik tehditler
- Temel sorumluluklar
- Fiziksel güvenlik nedir, ne değildir?
- Bilgisayar güvenliği için dikkat edilmesi gerekenler
- Parola güvenliği nasıl sağlanır?

# İÇERİK

- Güvenli olmayan yazılımlar nelerdir ve korunmak için neler yapılmalıdır?
- E-posta güvenliği
- Yedekleme
- Bilgi sınıflandırma ve etiketleme
- Sosyal mühendislik yöntemleri ve dikkat edilmesi gerekenler
- Güvenli internet
- Yasal sorumluluklar
- Bilgi güvenliği ihlal olayları
- Sistemin devamlılığının sağlanması

# Bilgi Nedir?

- Karar verme aşamasında kullanılan, **anlam taşıyan**, **işlenmiş** ve **analiz** edilmiş veriye **bilgi** denir. Bilgi, farklı ortamlarda farklı formatlarda bulunabilir.
- Süreçlerin devamlılığı için gerekli olan ve bu nedenle değeri olan, dolayısı ile uygun şekilde **korunması** gereken bir varlıktır.

# Bilgi

- ✓ Basılı halde kağıtlarda
- ✓ Elektronik dosyalarda
- ✓ Veritabanlarında
- ✓ Telefon konuşmalarında
- ✓ Faks mesajlarında
- ✓ Masalarda
- ✓ Dolaplarda
- ✓ İletim hatlarında
- ✓ Mobil uygulamalarda
- ✓ Kişilerin akıllarında

# Bilginin Özellikleri

Gizlilik (Yetkisiz kullanıcılar göremesin)

Bütünlük (Bilgi durduğu yerde bozulmasın)

Erişilebilirlik (Yetkili kullanıcılar görebilsin)

Gizlilik x Erişilebilirlik: Gizliliği korumak için alınan önlemler erişilebilirliği “bozar”

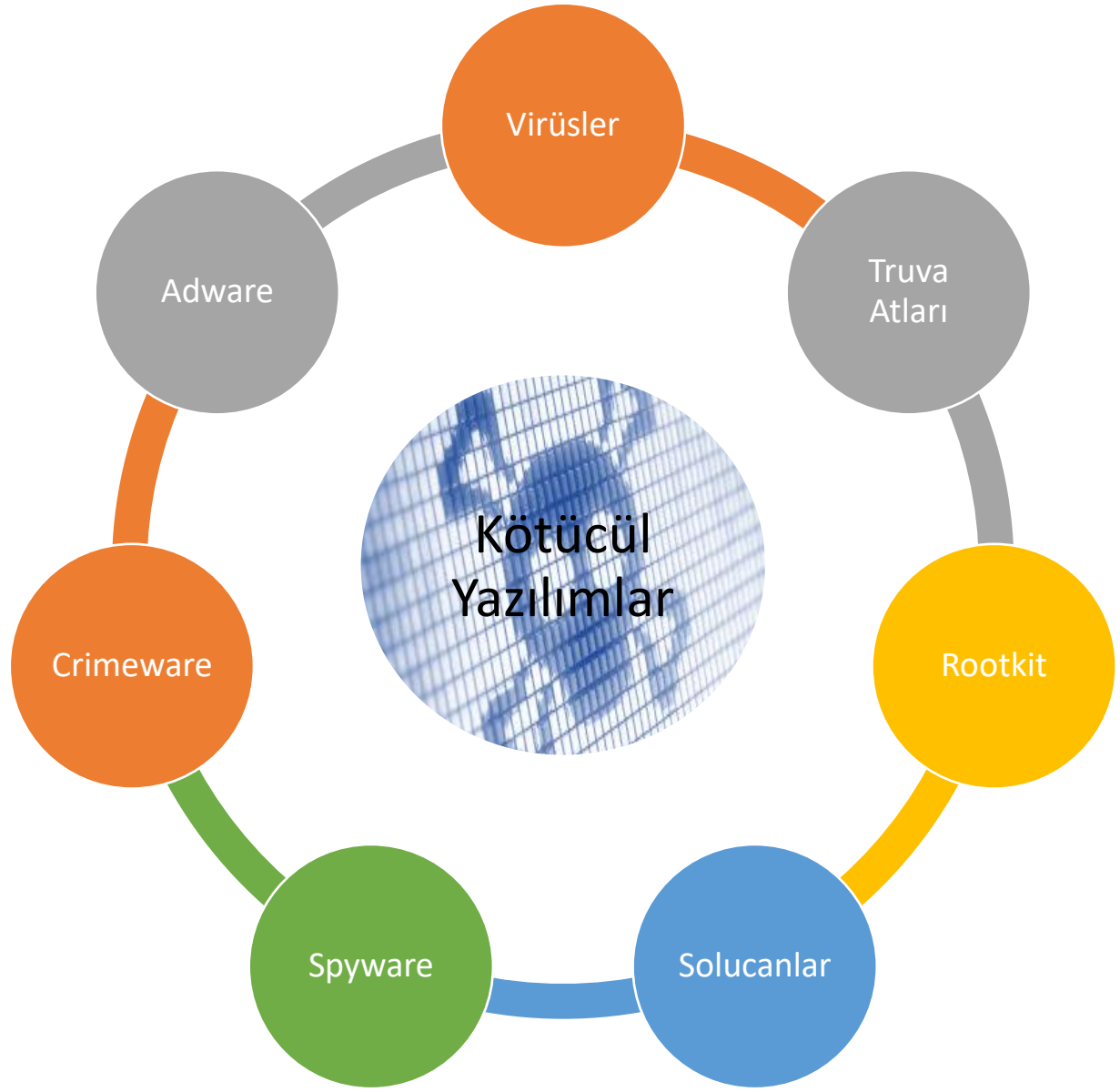
# Bilgi güvenliği

Kurumun en değerli varlığı olan Bilgi'nin kaybolmasını, zarara uğramasını, yok olmasını, yetkisiz ve **kötü niyetli** kişilerin **eline geçmesi**ni engellemektedir.

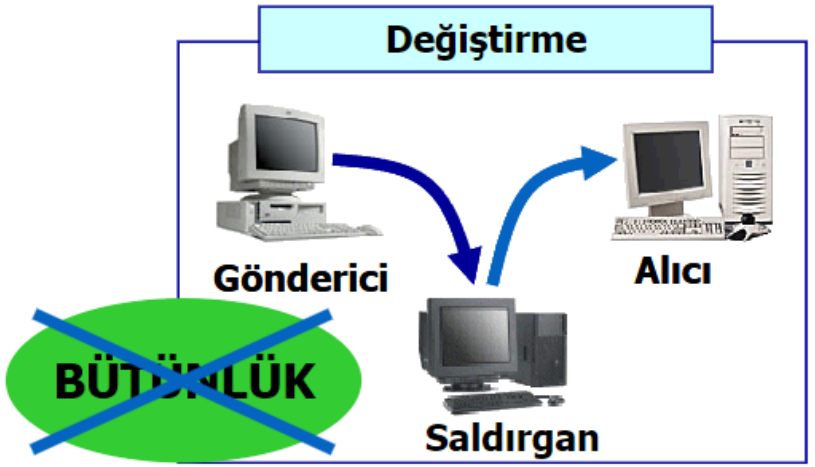
- Veri bütünlüğünün korunması
- Yetkisiz erişimin engellenmesi
- Mahremiyet ve gizliliğin korunması
- Sistemin devamlılığının sağlanması

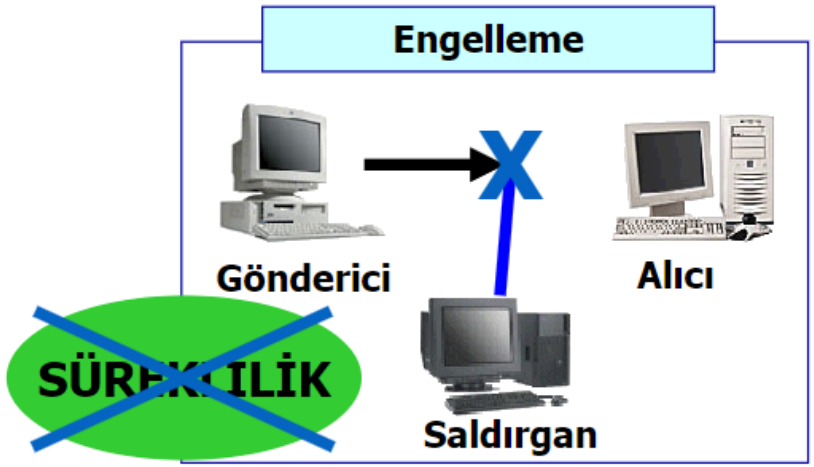
# Kötücül Yazılımlar

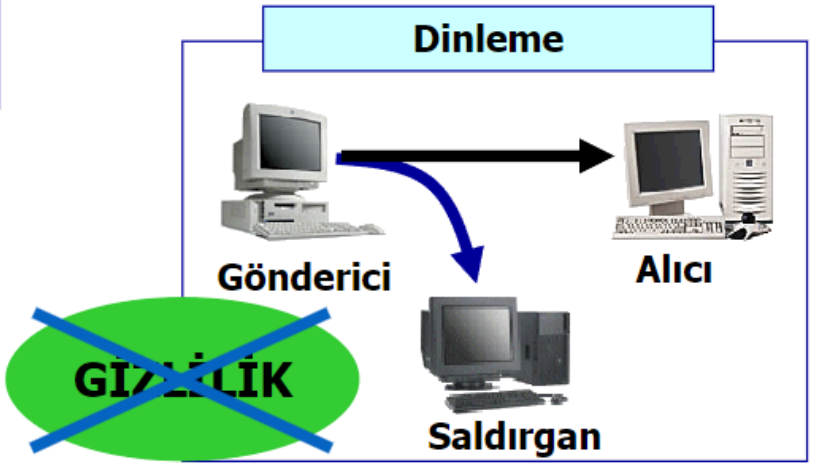
- Bir bilgisayarı veya içindeki bilgiyi sömürmek için tasarlanmış yazılımdır.
- Pek çok türü vardır:

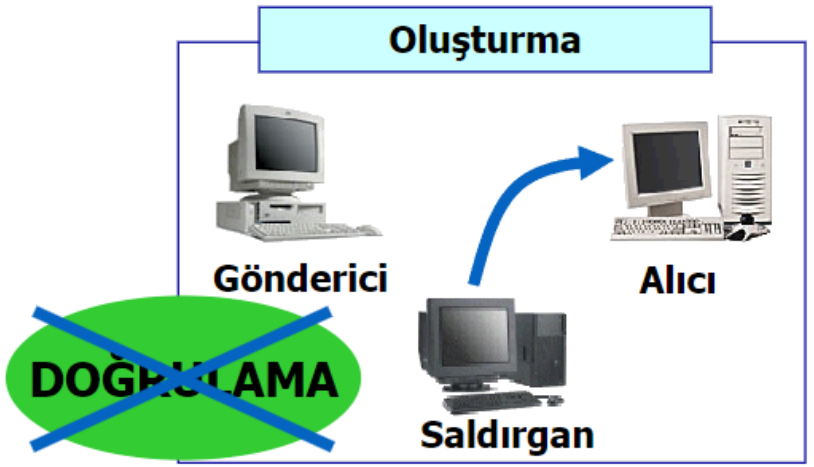


# Elektronik Tehditler

# Oluşabilecek Zararlar

- Önemli veriye zamanında erişememek
- Parasal kayıplar
- Vakit kayıpları
- Bilgileriniz başkalarının eline geçebilir.
- Kurumun onuru, toplumdaki imajı zarar görebilir. (en kötü durum)
- Donanım, yazılım, veri ve kurum çalışanları zarar görebilir.

# KURUMA AİT HASSAS BİLGİLER ÇALINABİLİR VEYA AÇIĞA ÇIKABİLİR

Örnek: HBO (ABD'nin önde gelen, paralı televizyon kanal grubudur) sunucuları ele geçirilerek Game of Thrones dizisi bölümleri çalınmış ve televizyon yayınlamadan torrent üzerinden yayınlamıştır.

1,5 TB'lık veri çalan bilgisayar korsanları (hacker), HBO'yu oyuncuların kişisel bilgilerini sızdırmakla tehdit etmişti.

# KURUMSAL İMAJ SARSILABİLİR

Örnek: 2013 ve 2014 yıllarında Yahoo firması veritabanı ele geçilerek 3 milyar kullanıcının verileri çalınmıştı. Yahoo gelmiş geçmiş en büyük veri hırsızlığına maruz kaldı.

Örnek: CCleaner uygulaması ele geçilerek içerisine virüs yerleştirilerek tahmini 2.27 milyon kişinin verisi çalınmıştı. Eğer kullandığınız sürüm 5.33 ise sizde etkilenmiş olabilirsiniz.


# İŞ SÜREKLİLİĞİ AKSAYABİLİR

**WannaCry** virüsü dünya çapında zarara neden olmuştur. Birçok otomobil firması **üretimi durdurmak** zorunda kalmıştır. Ülkemizde Ford bu saldırılardan etkilenen firmalardan biridir.

**Sabit diskleri şifreleyerek**

kullanıcıdan şifreyi kaldırma karşılığı ücret talep etmektedir.

# PARA VE DEĞER KAYIPLARI OLUŞABİLİR

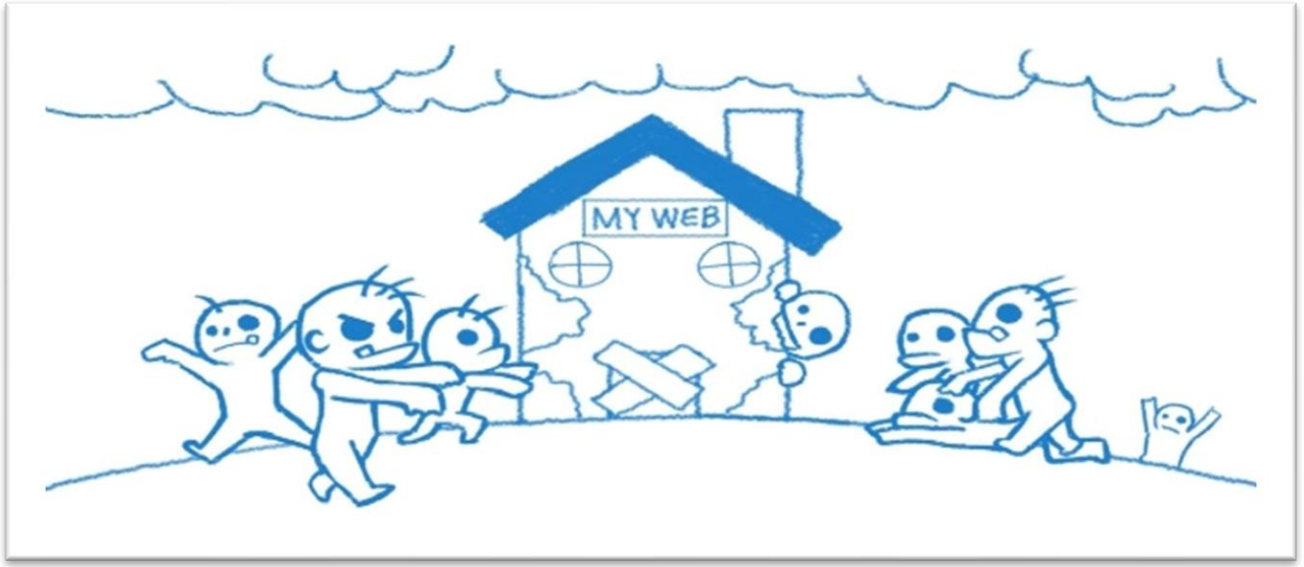
NiceHash firması büyük bir Bitcoin(kripto para) havuzu firması, 2017 yılında hacklenerek 4736 Bitcoin çalınmıştır. Firma yaklaşık 70 milyon dolar zarar etmiştir.

Kripto paralarda, para transfer edilen cüzdanların yeni olması nedeniyle, hesap geçmişinden suçluyu izlemek mümkün olmamaktadır.

# YASAL YAPTIRIMLARLA KARŞILAŞILABİLİR

Genellikle ‘‘Bot Bilgisayar’’ yada ‘’Zombi Bilgisayar’’ olarak adlandırılan ve bilgisayarınıza yerleşen virüsler sizin bilgisayarınızdan saldırgan tarafından belirlenen adreslere saldırı düzenler.

Bu nedenle yasal yaptırımlara maruz kalınabilir.



# ELEKTRONİK ORTAMDA SİZİN ADINIZA İŞLEM YAPILABİLİR

Özellikle şifresi çalınan sosyal medya hesaplarından arkadaşlara mesaj göndererek para isteme olayları sıklıkla rastlanan vakalardır.

# SİBER SAVAŞLAR

BT sistemlerine yapılan saldırıların yoğunluk, saldırı tipleri, amaçları ve nedenleriyle çok fazla çeşitlik kazandığı günümüzde, organize bir şekilde düzenlenen ve adına "Siber Savaşlar" denilen **uluslararası çapta büyük saldırılar** dönemi yaşanmaktadır.

**Ülkelerin ticari, ekonomik, sivil ve askeri sistemlerinin** kontrolleri büyük ölçüde dijital ortam üzerinde olması nedeniyle bu siber saldırılara karşı güvenlik önlemleri geliştirme ihtiyacı her geçen gün artmaktadır.

Siber Saldırıların **sebepleri** incelendiğinde;

- **Bir devlete, kuruma, ya da çeşitli güç merkezlerine tepki göstermek,**
- **Bilgi casusluğu yaparak çıkar sağlamak ,**
- **Güç gösterisi yaparak sesini duyurmak,**
- **Hedef bir kitlenin çalışmalarını engellemek**

gibi sebeplerle yapılmakta olduğu gözlenmektedir.

# Yanlış Fikirler

- Güvenlikten bilgi işlem sorumludur!
- Kurumumuz güvenlik duvarı (firewall) kullanıyor, dolayısıyla güvendeyiz!
- Dikkat!!! Bir çok güvenlik saldırısı kurum dışından gelmektedir!

# Kullanıcı Bilincinin Önemi!

- Bilgi güvenliğinin **en önemli** parçası **kullanıcı güvenlik bilinci**dir.
- Oluşan güvenlik açıklıklarının büyük kısmı **kullanıcı hatasından** kaynaklanmaktadır.
- Saldırganlar (Hacker) çoğunlukla **kullanıcı hatalarını** kullanmaktadır.
- Sosyal mühendislik içerikli **bilgi edinme girişimleri** yaşanmaktadır.

# Kullanıcı Sorumlulukları

- Bilgi güvenliğini sağlamak **sadece bazı birimlerin sorumluluğunda değildir**!

- Bilgi Güvenliğini sağlamak;

**TÜM ÇALIŞANLARIN SORUMLULUĞUNDADIR.**

- Saldırganlar çoğunlukla **kullanıcı hatalarını** kullanmaktadırlar.

# Bilgi güvenliğinin seviyesini en zayıf halka belirler.

# Neler Yapabiliriz?

| Güvenli Bilgisayar (Secure Laptop) | Güvenli Logon (Secure Logon) | Gündelik Siber Hijyen | Ev/İş ağınızı güvenli hale getirin |
|---|---|---|---|
| TPM (Tercihen v2.0)<br>Disk Şifreleme<br>Secure boot<br>İşletim Sistemi Güncellemeleri<br>Driver Güncellemeleri<br>Uygulama Güncellemeleri | BIOS Parolası<br>Başlangıç (Startup) Parolası<br>Multi-Faktör Doğrulama Yöntemleri<br>Uygulama Güncellemeleri | Parolanızı gönderirken dikkatli olun<br>VPN olmadan public Wi-Fi kullanmayın<br>Eğer SSL kilidi kırıksa bağlantı kurmayın<br>Bilgisayarınızın ekranı kilitli şekilde bırakmayın, işiniz bitince kapatın. | Kablosuz ağınızda düzgün güvenlik önlemlerini alın<br>Firmware güncellemesi yapılmamış aşağıdaki cihazları şahsi ağınıza dahil etmeyin<br>– Network Yazıcılar<br>– NAS Cihazlar<br>– Smart Home cihazlar<br>– Ethernet over power switches |

# FİZİKSEL GÜVENLİK

Bir varlık için uygulanan etkin fiziksel tedbirler olmadığı sürece diğer tedbirlerin etkinliği çok fazla olmayacaktır.

- Yetkili kişinin odada bulunmadığı zamanlarda oda **kilitli** tutulmalıdır.
- Anahtar personelde ve yedek anahtar **da ilgili birim amirinde** olmalıdır.
- CD, sarf malzemesi, sarf donanımlar vb. malzemeler mutlaka **kilitli ortamlarda** bulunmalıdır.
- Yetkisiz kişilerin ortama erişimleri **kontrollü** olmalıdır.

# FİZİKSEL GÜVENLİK


Alınan fiziksel önlemler etkili ve **varlığın amacına hizmet** etmesini engelleyen önlemler alınmamalıdır.

# PAROLA GÜVENLİĞİ

# PAROLA GÜVENLİĞİ


- Parolanız, size özel olan bilgilerle diğer kişiler arasındaki **en önemli güvenlik** önlemidir.
- Kişisel hesaplarla yapılan işlemlerin kayıt altına alınması ve bağlayıcı olması sebebi ile önem arz etmektedir.
- Kişisel olmayan bilgisayarlarda parola hatırla özelliği kullanılmamalıdır.
- Kişisel bilgisayarlarda parola hatırlatması kullanacaksa tüm parolalar için ana bir şifre belirlenmelidir.

# PAROLA GÜVENLİĞİ

- Kurum bünyesinde kullanılan parolalar ile diğer sitelerde (Facebook, Google, Twitter vb.) kullanılan **parolaların aynı olmaması** gerekmektedir.
- Özellikle **doğum günü**, **ardışık sayılar** ve ardışık harfler gibi parolalar **çok zayıf** parolalardır.
- Örnek zayıf parolalar: 123456, 09051976, telatyaka, abcde, ali1979 vb.

# PAROLA GÜVENLİĞİ

- Oluşturulan bir parolanın "**güçlü**" kabul edilebilmesi için aşağıdaki özellikleri göstermelidir.
- **En az 8** karakterden oluşmalıdır.
- Harflerin yanı sıra, rakam ve **"?, @, !, #, %, +, -, *, %"** gibi **özel karakterler** içermelidir.
- Büyük ve küçük harfler bir arada
- kullanılmalıdır.

# PAROLA GÜVENLİĞİ

- Kurumda kullanılan parolalar en az **8** karakterli olmalı**, büyük-küçük harf** ve **rakam** içermelidir.
- Parolalar ismin tamamını içermemelidir.
- Kurumdaki parola sistemine göre şifreler 90 günde bir değiştirilmelidir ve son kullanılan 8 parola kullanılmamalıdır.

# PAROLA GÜVENLİĞİ

**Parola kırılma süreleri**

- Uzunluk : 6 karakter
- Küçük harf : 10 dk.
- Küçük ve büyük harf :10 saat
- Küçük harf + büyük harf + rakamlar + sembol : 18 gün

**Parola kırılma süreleri**

- Uzunluk : 8 karakter
- Küçük harf : 4 gün
- Küçük ve büyük harf : 3 yıl
- Küçük harf + büyük harf + rakamlar + sembol : 463 yıl

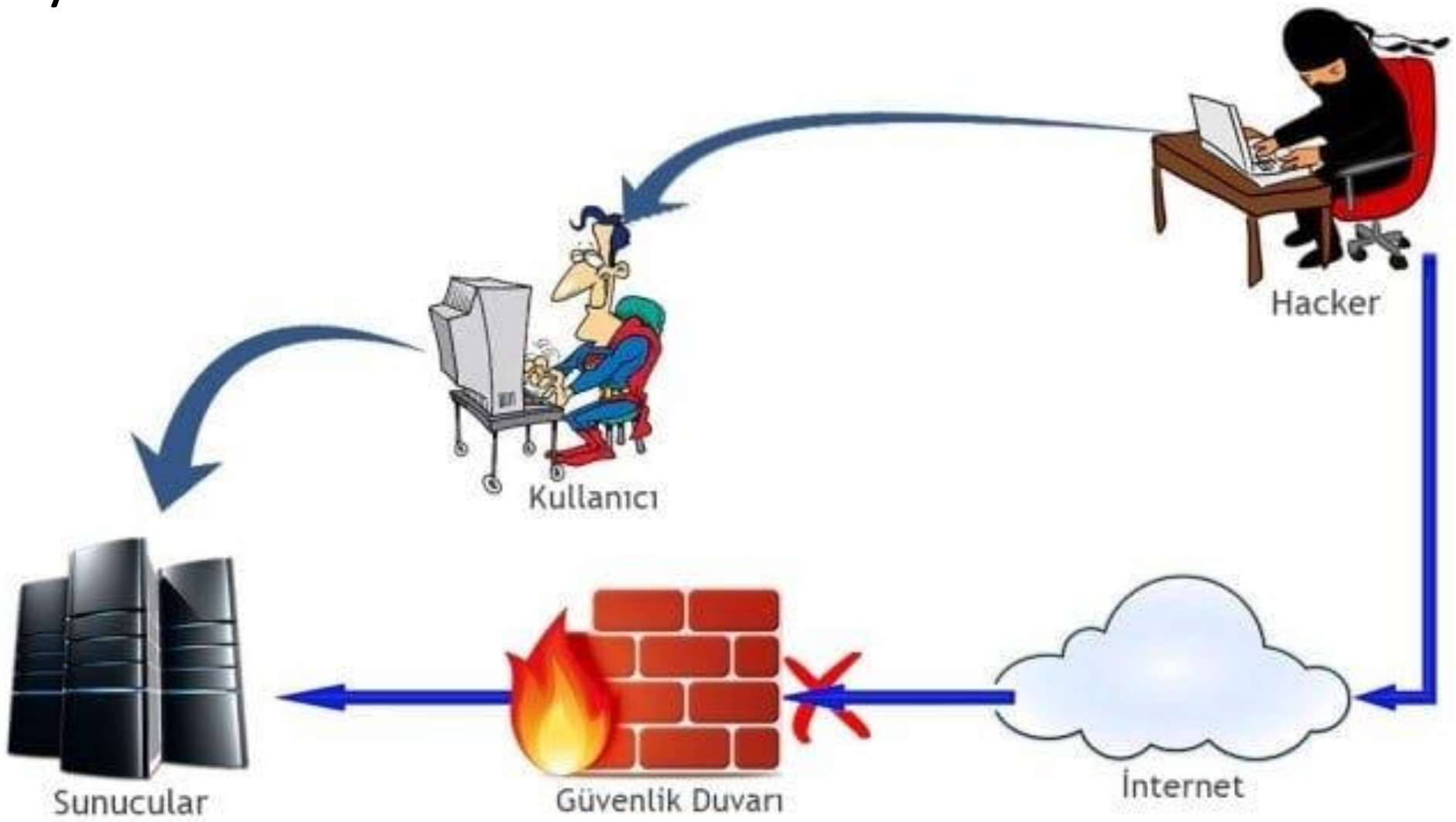
# PAROLA GÜVENLİĞİ

| Karakter Sayısı | Sadece Sayı | Küçük Harfler | Büyük ve Küçük Harfler | Sayılar, Büyük ve Küçük Harfler | Sayılar, Büyük ve Küçük Harfler, Semboller |
|---|---|---|---|---|---|
| 4 | Anında | Anında | Anında | Anında | Anında |
| 5 | Anında | Anında | Anında | Anında | Anında |
| 6 | Anında | Anında | Anında | Anında | Anında |
| 7 | Anında | Anında | 1 saniye | 2 saniye | 4 saniye |
| 8 | Anında | Anında | 28 saniye | 2 dakika | 5 dakika |
| 9 | Anında | 3 saniye | 24 dakika | 2 saat | 6 saat |
| 10 | Anında | 1 dakika | 21 saat | 5 gün | 2 hafta |
| 11 | Anında | 32 dakika | 1 ay | 10 ay | 3 yıl |
| 12 | 1 saniye | 14 saat | 6 yıl | 53 yıl | 226 yıl |
| 13 | 5 saniye | 2 hafta | 332 yıl | 3k yıl | 15k yıl |
| 14 | 52 saniye | 1 yıl | 17k yıl | 202k yıl | 1mil yıl |
| 15 | 9 dakika | 27 yıl | 898k yıl | 12mil yıl | 77mil yıl |
| 16 | 1 saat | 713 yıl | 46mil yıl | 779mil yıl | 5myr yıl |
| 17 | 14 saat | 18k yıl | 2myr yıl | 48myr yıl | 380myr yıl |
| 18 | 6 gün | 481k yıl | 126myr yıl | 2tn yıl | 26tn yıl |

# Sosyal Mühendislik

- İnsan faktörünü kullanan saldırı tekniklerinden ya **da kişiyi etkileme** ve **ikna** yöntemlerinden faydalanarak normal koşullarda bireylerin gizlemeleri / paylaşmamaları gereken bilgileri bir şekilde ele geçirme sanatı **Sosyal mühendislik** olarak ifade edilir.

# Sosyal Mühendislik



# Sosyal Mühendislik Teknikleri

- Omuz Sörfü
- Çöp Karıştırma
- Truva Atı
- Rol Yapma
- Tersine Sosyal Mühendislik
- Oltalama

# İnsan Davranışları

Her Sosyal Mühendis maksimum bilgiye ulaşabilmek için kurbanın belli davranış özelliklerine kilitlenir.

# Omuz Sörfü

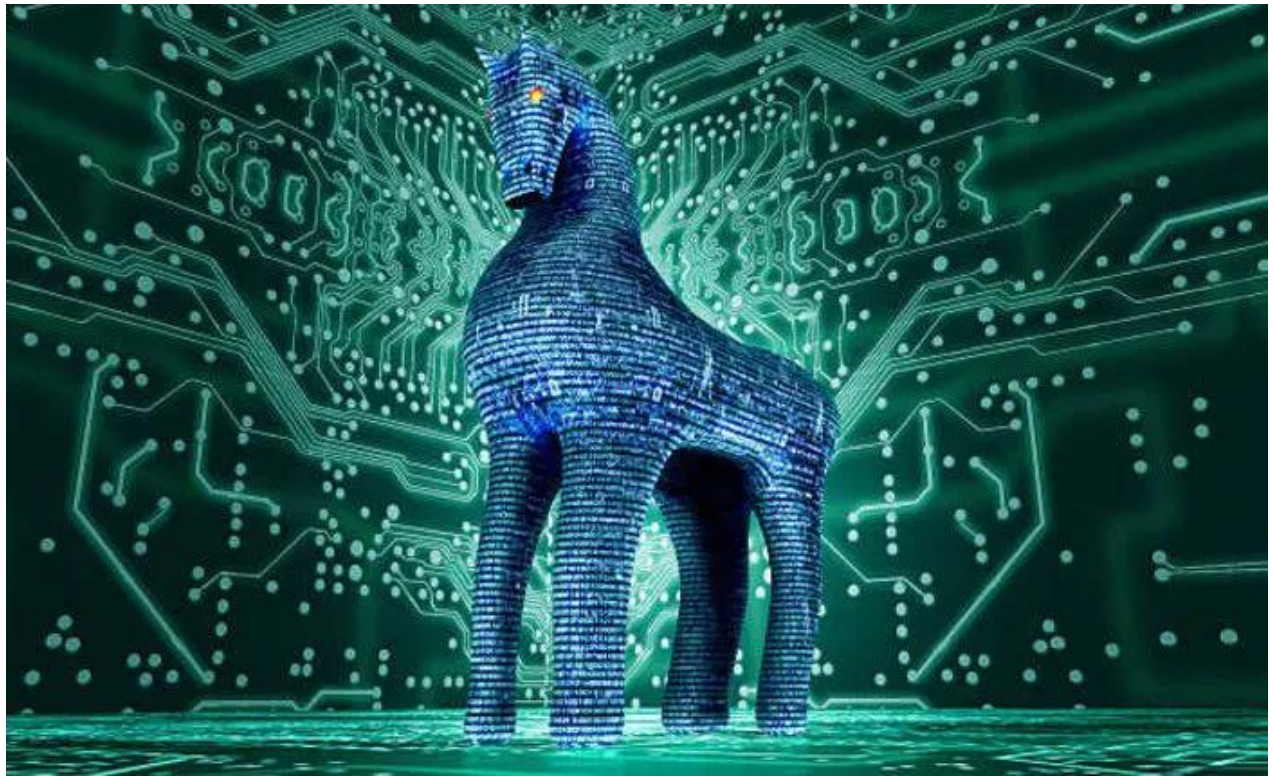
- Parola ile erişim olan herhangi bir sisteme erişim sağlarken kullanıcının izlenmesidir
- Genellikle kurum dışında, kafe, havalimanı, otel gibi yerlerde yapılır.
- Her zaman tesadüf olmaz.

# Çöp Karıştırma

- Önemsiz gibi görünen bilgiler kullanarak inandırıcı senaryolar hazırlamakta kullanılır.
- Önemsiz görünen belgeler,
- Flaş disk, CD gibi veri içeren materyaller,
- İmla hatasından atılan raporlar,
- Notlar ve telefon numaraları.

# Truva Atı

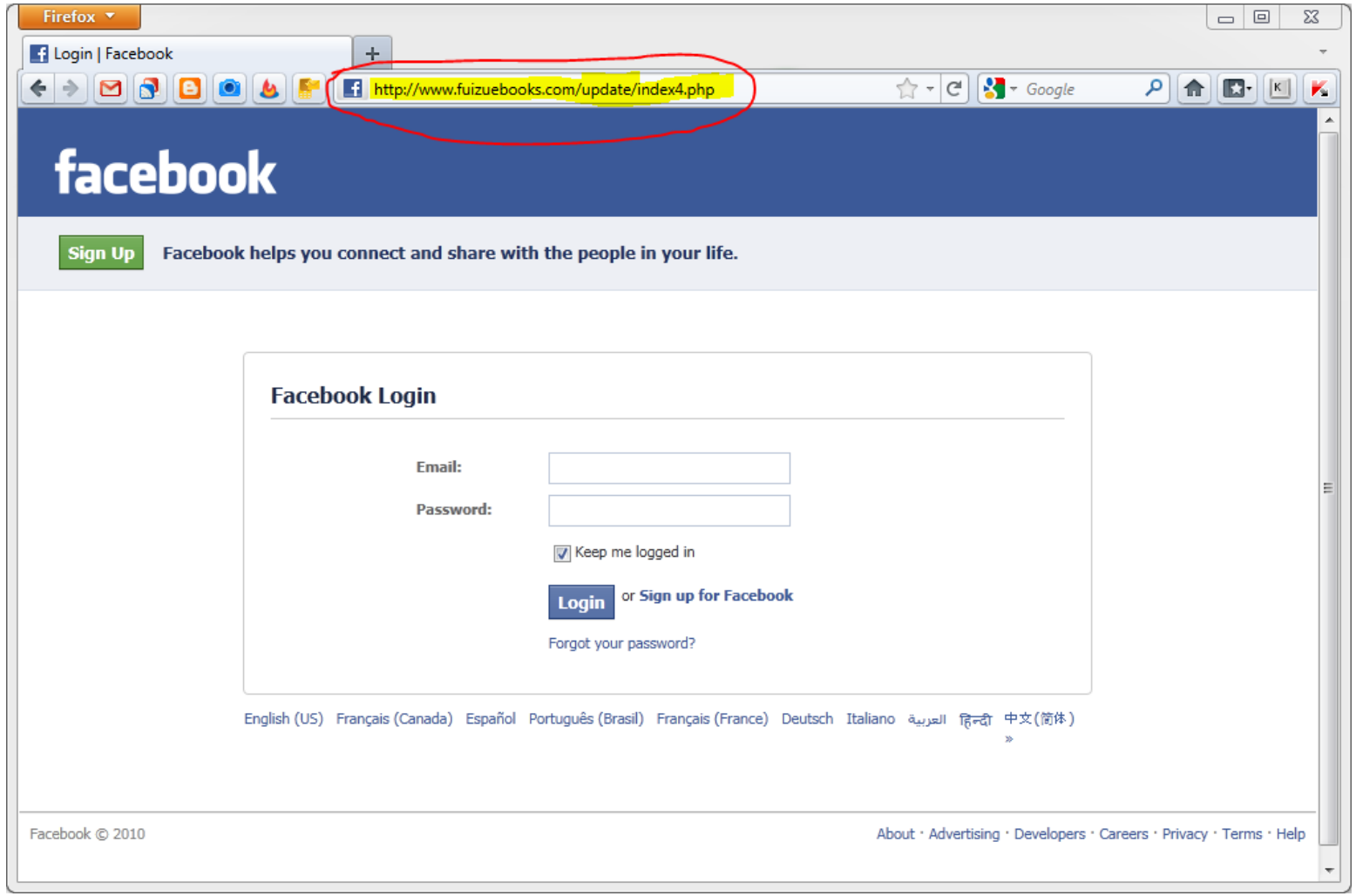
- Zararsız gibi görünür.
- Oyunların kırılması için gerekli uygulamalarda bulunabilir.
- Güvensiz kaynaktan yayınlanıyor olabilir.



# Rol Yapma

- Dolandırıcılıkta günümüzün en yaygın kullanım şeklidir. Telefonla arayarak kendisinin **banka**dan aradığını ya da **polis** olduğunu söyleyerek hassas bilgilere erişim sağlamak istemektedir. Bu tip kişiler aradıkları kişi ile ilgili **geniş bilgiye** sahiptir.

# Sosyal Mühendislik



# Tersine Sosyal Mühendislik

- Rol yapma tekniğine benzerdir fakat bu sefer kurban yardım istemektedir. 3 adımdan oluşur:
- **Sabotaj:** Sistem bozarak kullanıcıyı yardım istemeye zorlar.
- **Pazarlama:** Sistemi düzeltmeyi teklif eder.
- **Destek:** Kurban sorunun çözülmesi için saldırgana istediği bilgi ve yetkiyi verir.

# Oltalama

- İletişim yolları kullanılarak yapılan bir saldırı türüdür. Eposta, SMS ve diğer mesajlaşma yazılımları.
- **SMS** ile **ödül** kazandığınızı ve linke tıklayarak alabileceğinizi söyler.
- Mesajlaşma yazılımlarından arkadaşlarınıza bulaşan virüsler kendini taşımak için size sahte adres gönderir.
- En sık kullanılanı **Eposta** yoludur.

# Oltalama

İnternet Şubemize Giriş Yapan
Müşterilerimiz ;
-90 İPhone X
-900 Samsung Galaxy Tab 3 LİTE
-9000 Kişiye 200 TL Bonus Puan . Detaylar
İnternet Şubemizde http://vakiftank.com/

# BİR SALDIRININ UYARI SİNYALLERİ

- Bir geri arama numarası vermekten kaçınılması.
- **Sıra dışı** taleplerde bulunulması.
- Yetkili olduğunu öne sürmesi.
- **Acil**liğin üzerine vurgu yapılması.
- İsteğin yerine getirilmemesi durumunda kötü sonuçlar doğacağının söylenmesi.
- Soru sorulduğunda rahatsız olunması.
- Bilinen adların sıralanması.
- İltifat edilmesi ve kur yapılması.

# Yasal Sorumluluklar

- Bilgi güvenliği zafiyetlerinin çok az bir kısmı teknik açıklıklardan kaynaklanmaktadır. Büyük çoğunluğu insan hatalarından ve bilinçsizlik nedeniyle oluşmaktadır.

Örn: kapıyı açık bırakmak, bilgisayarı kilitlememek, parola paylaşmak vb.

# Bilgi Güvenliği İhlali

- İnternet’te **uygunsuz içerik** veya **suç unsuru** içeren yayınlar fark ettiğiniz zaman bunları ilgili kurum ya da birimlere **bildirmeniz** gerekir.
- Uygunsuz veya suç unsuru içeren internet yayınlarını Telekomünikasyon İletişim Başkanlığı'nın kurduğu **İnternet Bilgi İhbar Merkezi**’ne bildirebilirsiniz.

BİTTİ ☺