Siber saldırı olduğunda ne yapılması gerekir?

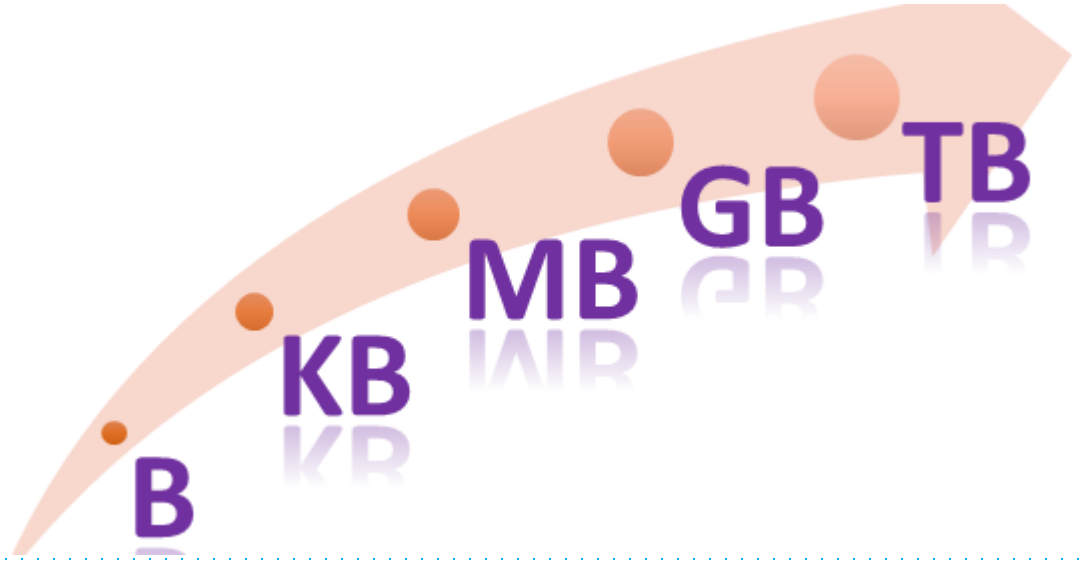
2025-2026

ÇAĞ ÜNİVERSİTESİ
ÇAĞ UNIVERSITY

BİLGİ GÜVENLİĞİ YÖNETİMİ

Dr. Öğr. Üyesi Taylan Tutkunca

MESLEK YÜKSEKOKULU

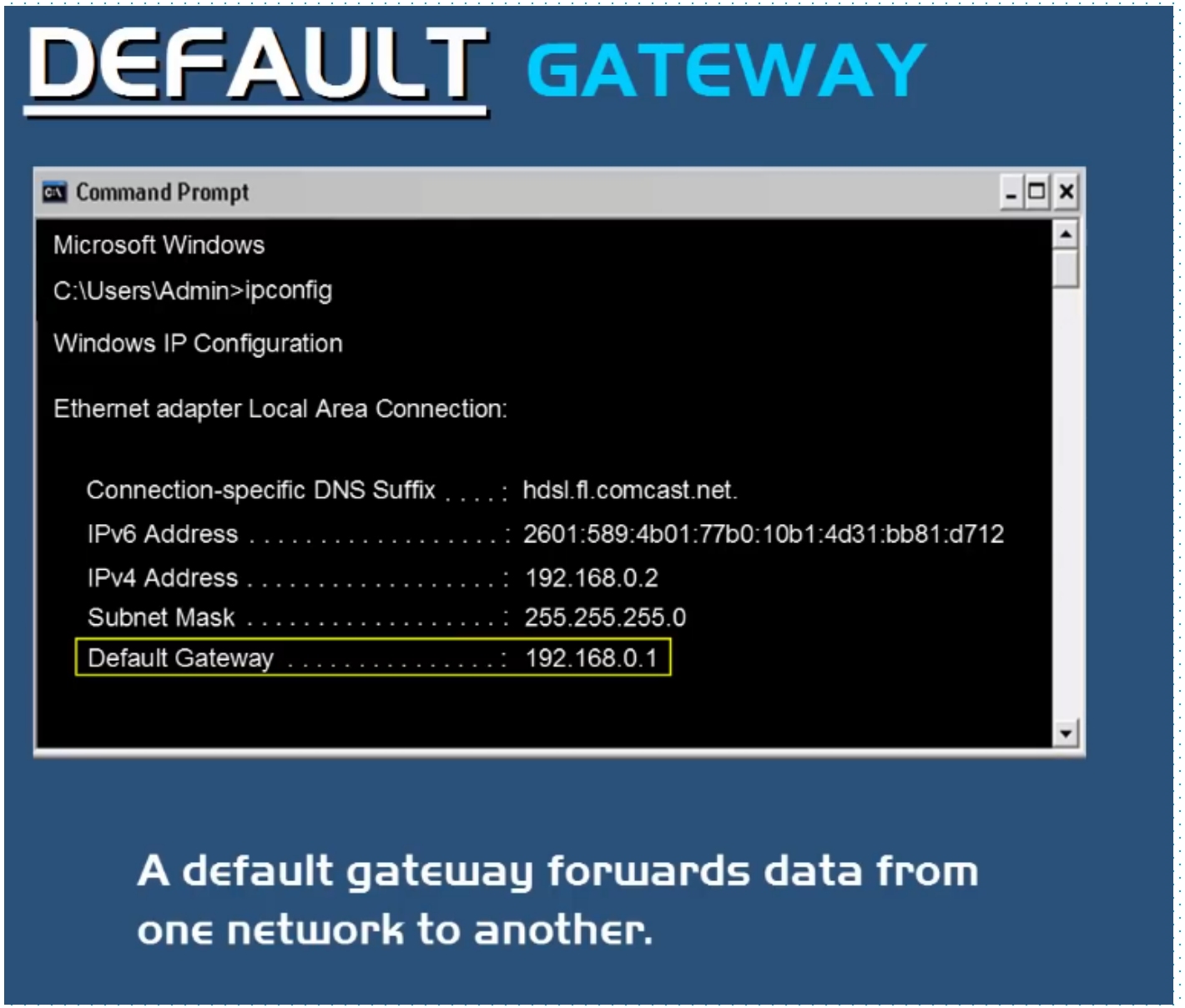


Veri Depolama Birimleri Eşitlikleri

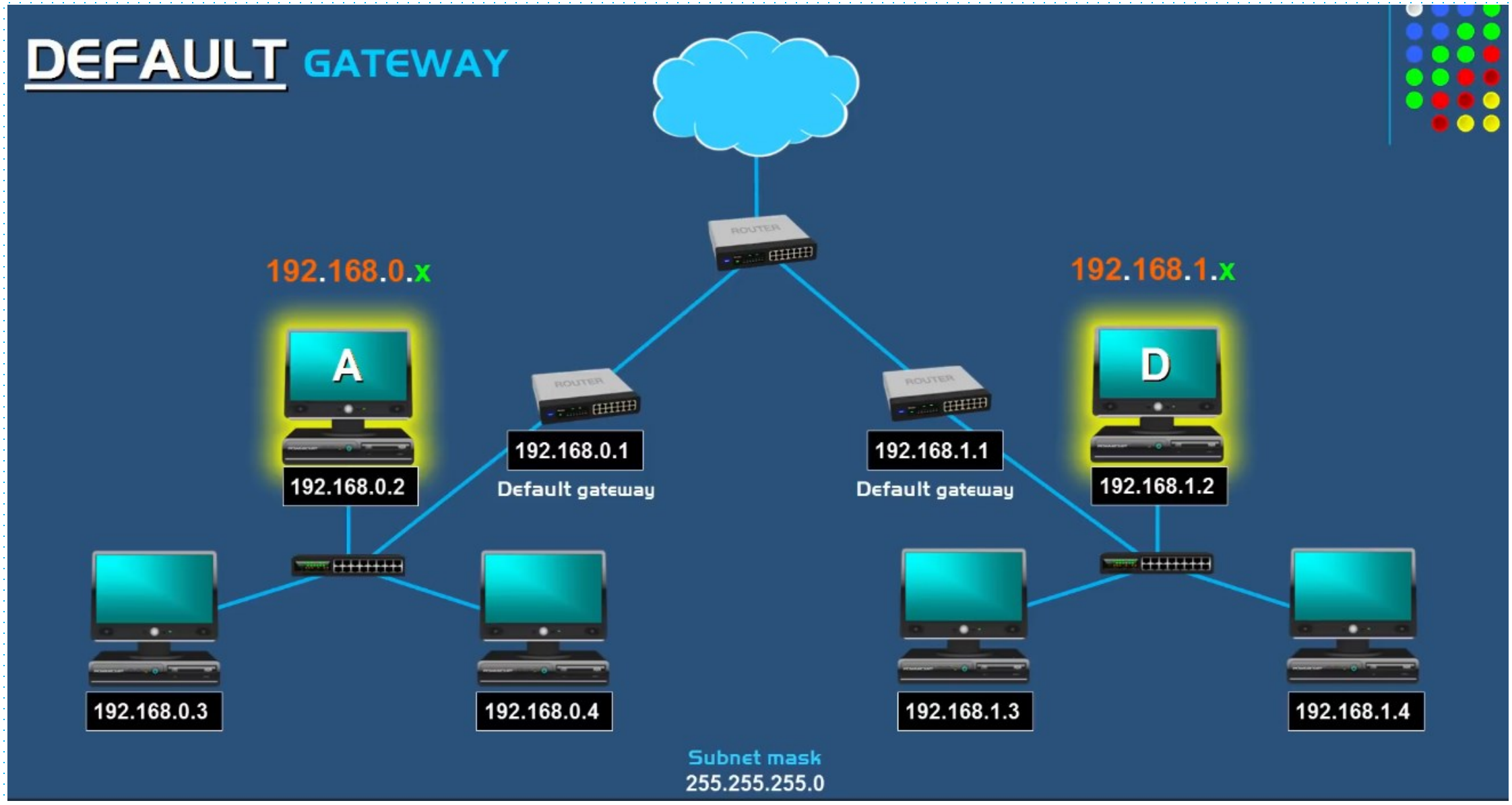
8 bit	=	1 Byte
1024 Byte	=	1 KB (KiloByte)
1024 KB	=	1 MB (MegaByte)
1024 MB	=	1 GB (GigaByte)
1024 GB	=	1 TB (TeraByte)
1024 TB	=	1 PB (PetaByte)
1024 PB	=	1 EB (ExaByte)
1024 EB	=	1 ZB (ZettaByte)
1024 ZB	=	1 YB (YottaByte)

- **IP adresi**, Internet'e bağlanacak olan her bilgisayar veya aygıtı benzersiz şekilde tanımlayan bir numaradır.

Ağ geçidi, bilgisayar ağlarında, başka bir ağa erişim noktası olarak hizmet veren bir adrestir. Bilgisayar ağında bulunan, bir IP adresi, yönlendirme tablosunda herhangi bir hatla eşleşmediği zaman bu adrese gider.

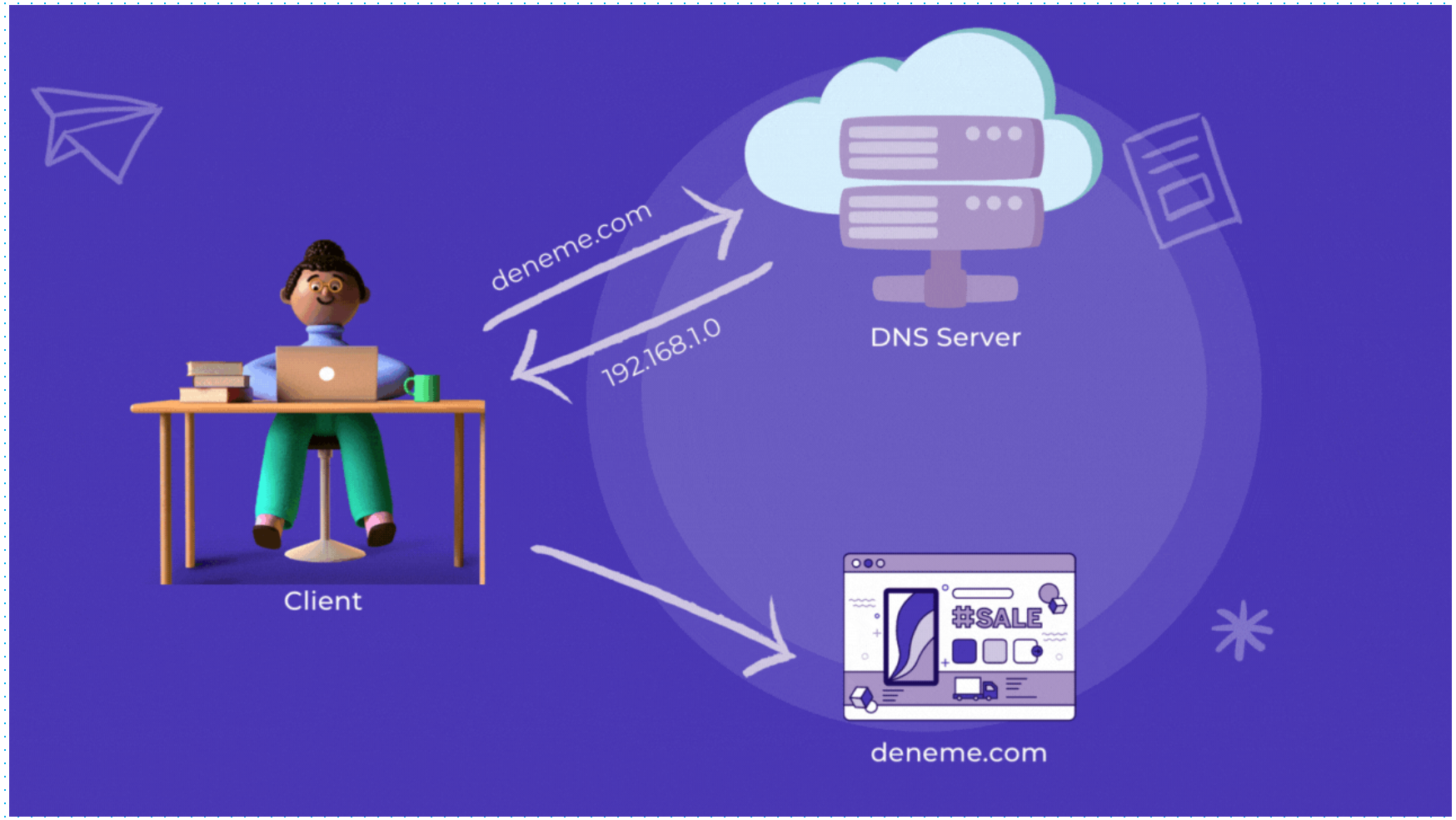


Bilgi Güvenliği



Alan adı, bir IP adresinin yazı ile ifadesidir.

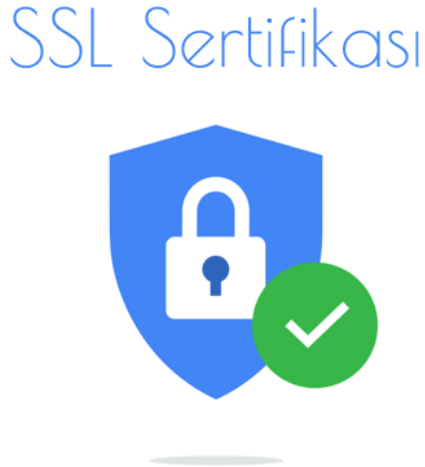
DNS sunucusu, alan adını ilişkili IP adresine dönüştürür



SSL Sertifikası

"Secure Sockets Layer" web site denildiği zaman, akla gelen hususlardan birisi.

SSL sertifikasına sahip bir web sitesinin uzantısı artık "http" olarak değil, "**https**" olarak görünür. Bu sonuna gelen "-s" takısı web sitenin güvenilir olduğunu belirtir.



Bilgi Güvenliği

Kullanıcı 1

HTTP

htttp://www.example.com

şifre : abc123

Şifreleme olmadan
korsanların gördüğü şifre “abc123”

Kullanıcı 2

HTTPS

htttps://www.example.com

şifre : abc123

Şifreleme varken
korsanların gördüğü şifre “xgeaDarz”

Bilgi Güvenliği

Sizin Şifreniz Ne Kadar Güvenli?

Bilgi Güvenliği

Günümüzde bilgi güvenliğinin sağlanması en temel kurumsal süreçlerden birisi olmasına rağmen…

Bilgi Güvenliği

Beklenilmeyen bir noktadan sorun çıkabilir…

Hacker kimdir?

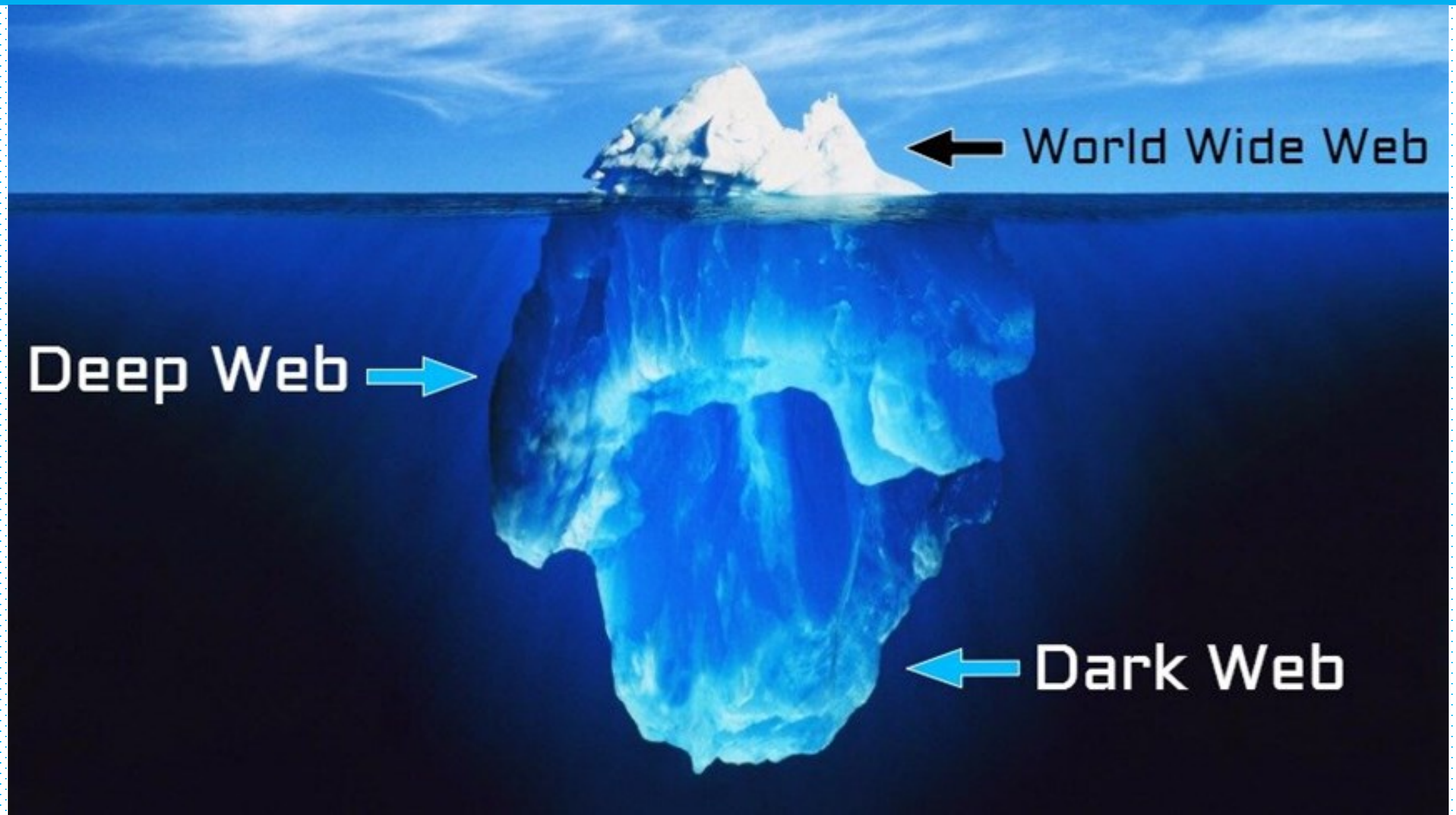
Bilgisayar teknolojileri alanında son derece yetenekli, yazılım dillerini bilen, son derece yaratıcı ve zeki kişilerdir. Yapılan saldırıları misyon edinir ve bundan zevk alır.

Lamer kimdir?

İnternet ortamında çocukça ve anlamsızca şeyler yapan ve hacker olmamasına rağmen kendini hacker olarak gösteren kişilere verilen isimdir.

Bilgi Güvenliği

Bilgi Güvenliği



Bilginin Önemi

- Bir devlete ait askeri, mali, enerji vb bilgileri
- Bir şirkete ait yatırım, borç-alacak bilgileri
- Bir üniversiteye ait AR-GE proje bilgileri
- Bir kişiye ait özel iletişim, harcama bilgileri
- Üst düzey kişilere ait sağlık bilgileri

Tüm bu ve benzeri bilgiler çok kritiktir. Rakip/düşmanların eline geçmesi büyük zararlar verir. Dolayısıyla korunması gerekir.

Siber Güvenlik

Kişilerin, kurumların, kuruluşların ve devletlerin bilgi varlıklarını ve kaynaklarını hedeflenen amaçlar doğrultusunda bilgi değerlerini dikkate alarak başlarına **KÖTÜ BİR ŞEYLER GELMEDEN** korumaktır.

TIMELINE OF THE WORST COMPUTER VIRUSES IN HISTORY

THE MOST DESTRUCTIVE AND NOTABLE COMPUTER VIRUSES AND WORMS

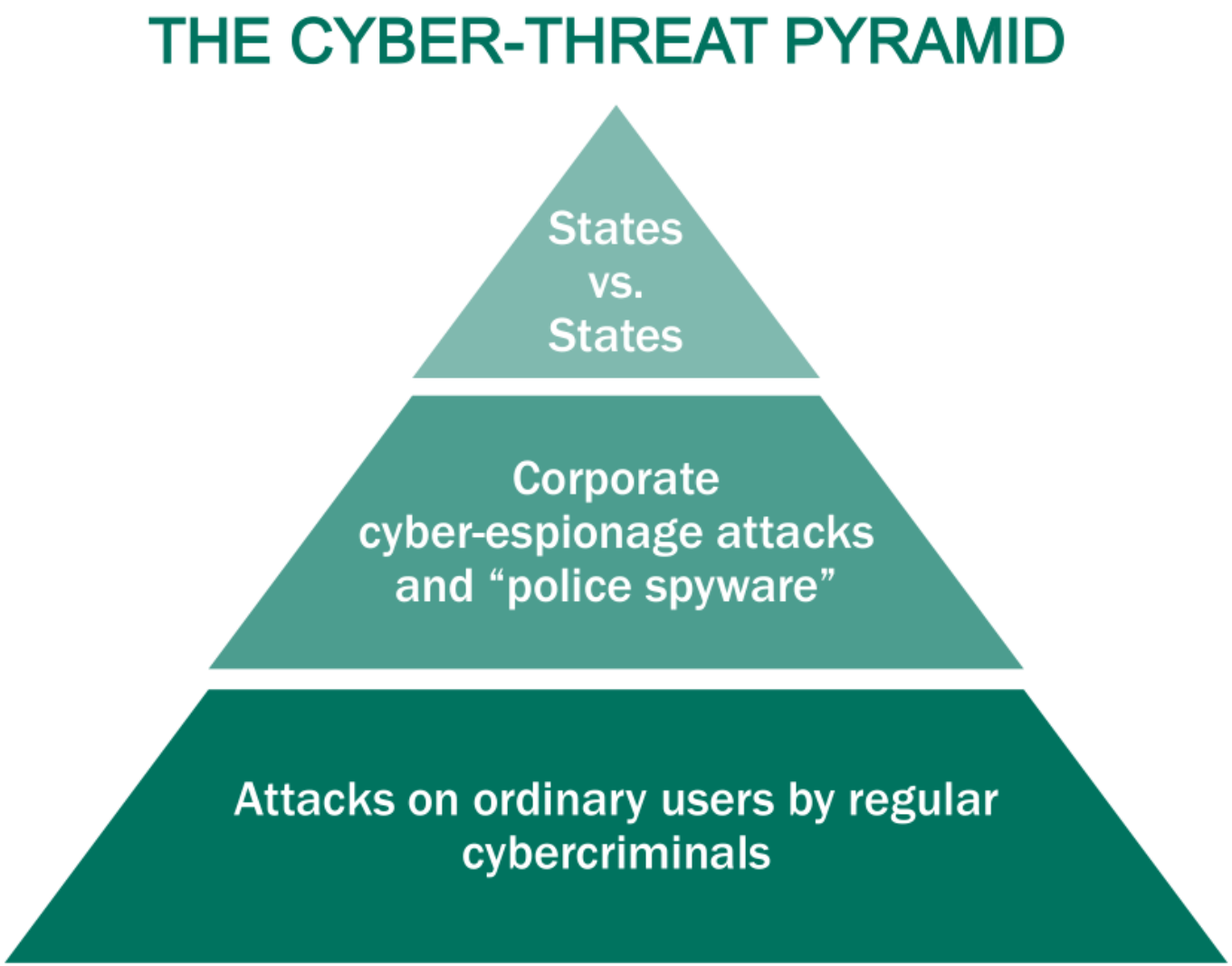
1971

CREEPER

Generally thought of as the first computer virus, Creeper was originally created as a security test to see if self-replicating programs were feasible. It did nothing malicious to computers that were infected.

1974

Bilgi Güvenliği



Siber Saldırı:

* Kişi, Şirket, Kurum, Örgütlerin *bilgi sistemlerine* veya *iletişim altyapılarına* yapılan **planlı** ve **koordineli saldırılar**
* Ticari, Politik veya Askerî Amaçlı

Siber Savaş:

* Aynı saldırıların Ülke veya Ülkelere yönelik yapılması

Buna göre;

* Anonymous'un Türkiye'deki bazı kurumlara yönelik eylemine **siber saldırı**,
* Wikileakes'in yaptığına ise **siber savaş** denebilir

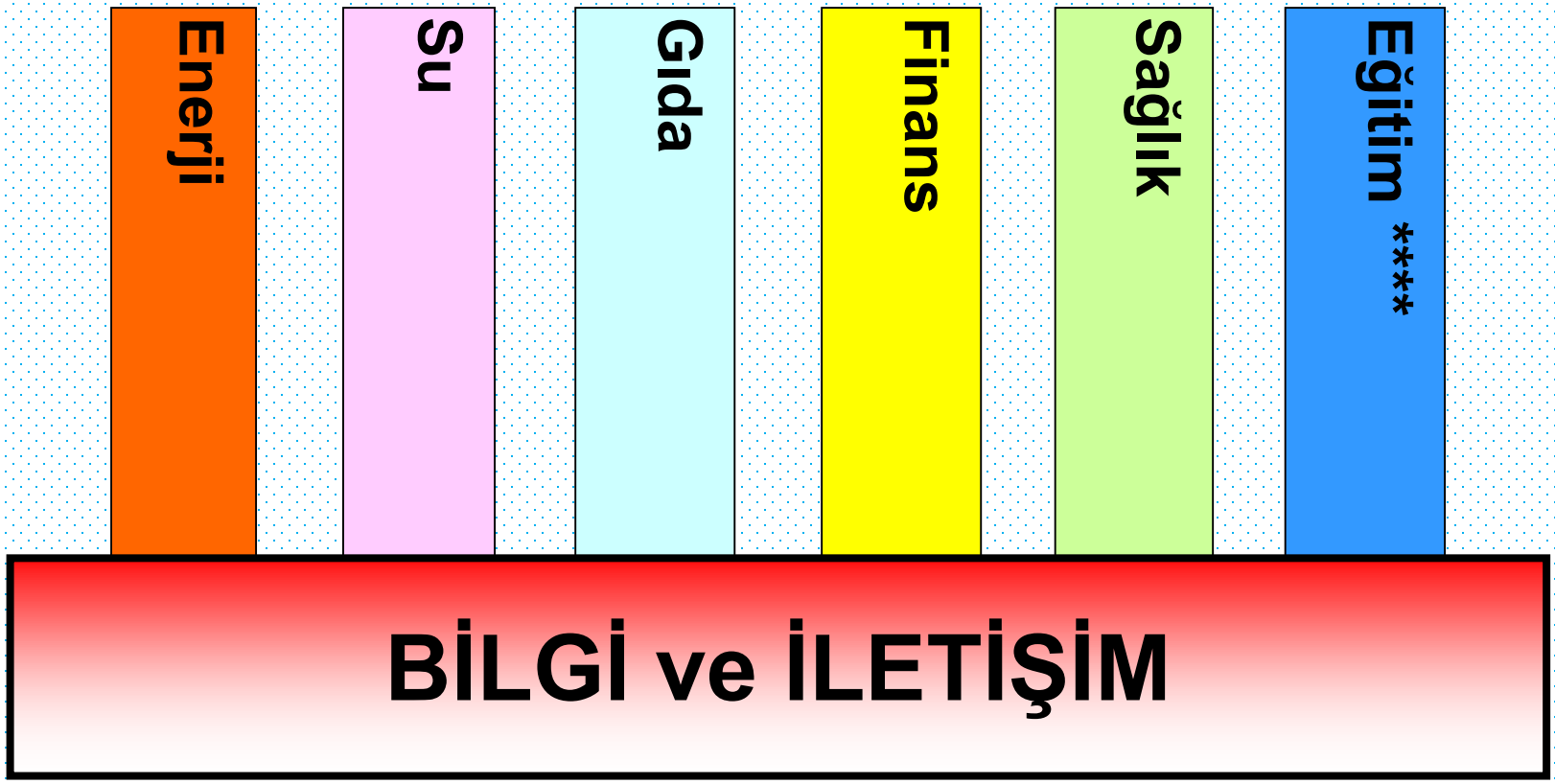
Devlet Destekli Siber Saldırılar

Devletler, siber kuvvetler tesis etmeye yönelmiştir

ABD, 2009'da Siber Savaş Komutanlığı'nı kurmuştur.

Çin, 2050 yılına kadar elektronik egemenliği hedeflemektedir ve bu kapsamda bir *siber doktrin* geliştirmiştir.

Kritik Altyapılar



Kaynak: Canbay, C., Kritik Altyapıların Korunması, CEBIT 2008

Türkiyeye Yapılan Saldırılar

- Cumhurbaşkanlığı
- TBMM
- Başbakanlık
- İçişleri/Dışişleri/Ulaştırma vb. Bakanlıklar
- Genel Kurmay Başkanlığı/MIT/Emniyet/BTK/TİB vb. Kurum ve Kuruluşlar

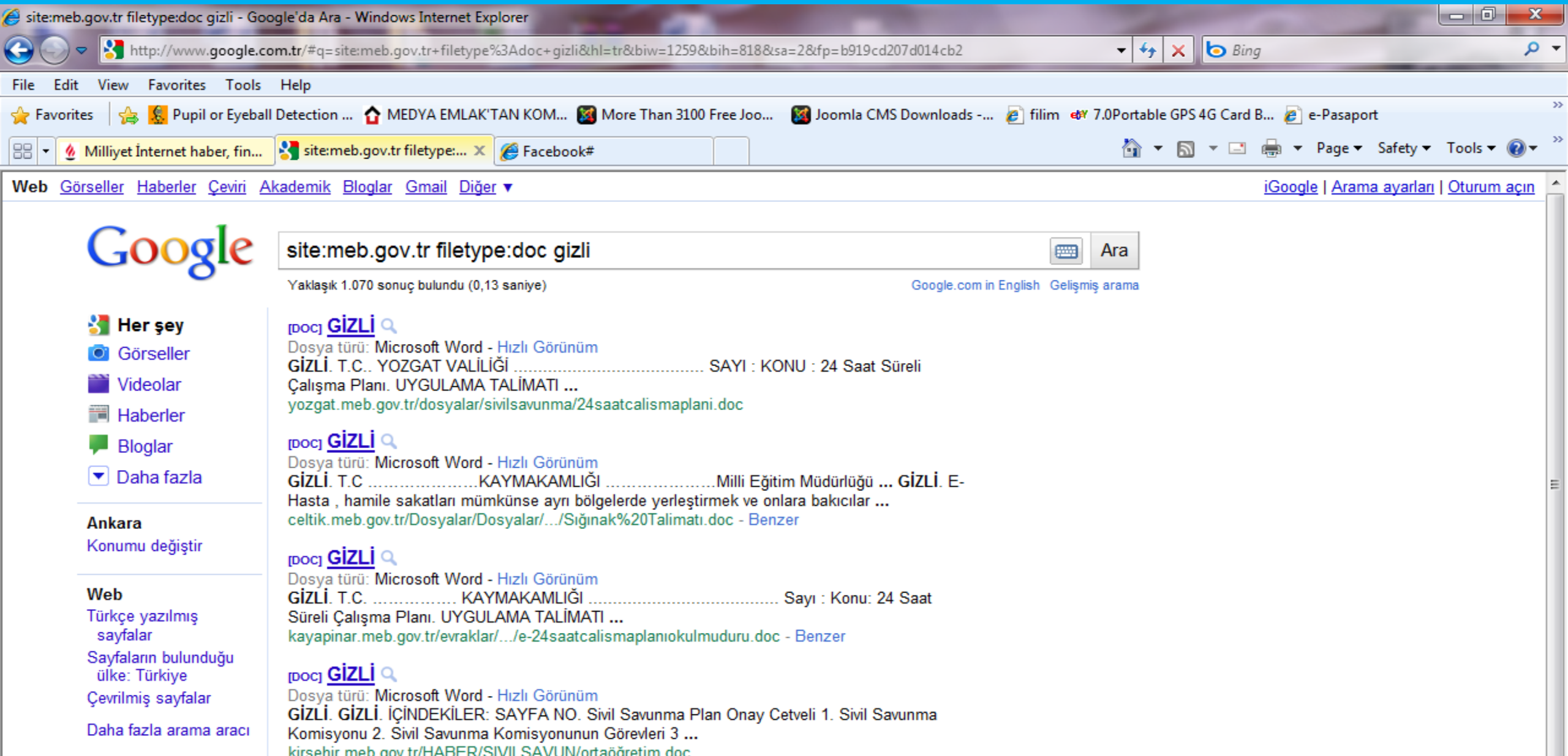
- Bilinmeyenler.?

GOOGLE

- Mükemmel bir arama motoru
- En çok tercih edilen arama motoru
- Mükemmel hizmetler veriyor
  - Academics, books, translation, blogs, gmail, documents, mobil, talk, maps, IPv6, Google+, ……
  - Değeri 200 Milyar Dolar
- FAKAT…

GOOGLE

- Dünyanın en iyi casus yazılım sistemi
- Dünyanın bilgisini topluyor..
- Ülkesine hizmet eden en iyi yazılımlardan birisi..
- Bizi bizden (ülkeleri, ülkelerden) daha iyi analiz edebiliyor..
- Kelime/Cümle/Resim/Ses araması yapabiliyor..
- İstihbarat için vazgeçilmez bir ortam..
- Tabii ki bu sistemi iyi kullananlar için..
- encrypted.google.com hizmete giriyor..
- Güvenlik açığı oluşturabilecek hususları kapatıyor..


site:meb.gov.tr filetype:doc gizli - Google'da Ara - Windows Internet Explorer
http://www.google.com.tr/#q=site:meb.gov.tr+filetype%3Adoc+gizli&hl=tr&biw=1259&bih=818&sa=2&fp=b919cd207d014cb2
File Edit View Favorites Tools Help
Favorites
Milliyet İnternet haber, fin...
site:meb.gov.tr filetype:...
Facebook#
Page Safety Tools
Web Görseller Haberler Çeviri Akademik Bloglar Gmail Diğer
iGoogle | Arama ayarları | Oturum açın
Google
site:meb.gov.tr filetype:doc gizli
Ara
Yaklaşık 1.070 sonuç bulundu (0,13 saniye)
Google.com in English Gelişmiş arama
Her şey
Görseller
Videolar
Haberler
Bloglar
Daha fazla
Ankara
Konumu değiştir
Web
Türkçe yazılmış sayfalar
Sayfaların bulunduğu ülke: Türkiye
Çevrilmiş sayfalar
Daha fazla arama aracı
[DOC] GİZLİ
Dosya türü: Microsoft Word - Hızlı Görünüm
GİZLİ. T.C.. YOZGAT VALİLİĞİ ..... SAYI : KONU : 24 Saat Süreli Çalışma Planı. UYGULAMA TALİMATI ...
yozgat.meb.gov.tr/dosyalar/sivilsavunma/24saatcalismaplani.doc
[DOC] GİZLİ
Dosya türü: Microsoft Word - Hızlı Görünüm
GİZLİ. T.C .....KAYMAKAMLIĞI .....Milli Eğitim Müdürlüğü ... GİZLİ. E-Hasta , hamile sakatları mümkünse ayrı bölgelerde yerleştirmek ve onlara bakıcılar ...
celtik.meb.gov.tr/Dosyalar/Dosyalar/.../Sığınak%20Talimatı.doc - Benzer
[DOC] GİZLİ
Dosya türü: Microsoft Word - Hızlı Görünüm
GİZLİ. T.C. ..... KAYMAKAMLIĞI ..... Sayı : Konu: 24 Saat Süreli Çalışma Planı. UYGULAMA TALİMATI ...
kayapinar.meb.gov.tr/evraklar/.../e-24saatcalismaplanıokulmuduru.doc - Benzer
[DOC] GİZLİ
Dosya türü: Microsoft Word - Hızlı Görünüm
GİZLİ. GİZLİ. İÇİNDEKİLER: SAYFA NO. Sivil Savunma Plan Onay Cetveli 1. Sivil Savunma Komisyonu 2. Sivil Savunma Komisyonunun Görevleri 3 ...
kirsehir.meb.gov.tr/HABER/SIVIL SAVUN/ortaöğretim.doc

ISO 27001
BİLGİ GÜVENLİĞİ

Bilgi Güvenliği

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

- Karar verme aşamasında kullanılan, **anlam taşıyan**, **işlenmiş** ve **analiz** edilmiş veriye **bilgi** denir. Bilgi, farklı ortamlarda farklı formatlarda bulunabilir.

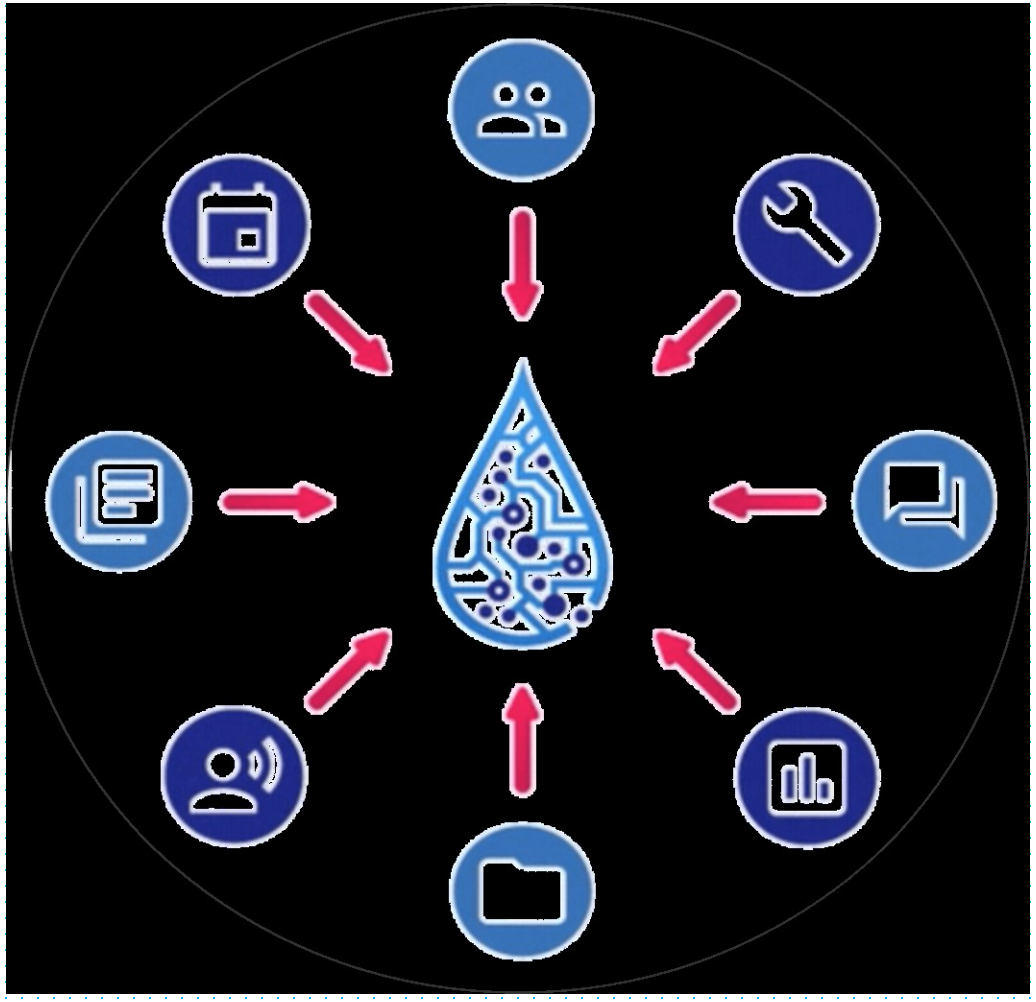
- Süreçlerin devamlılığı için gerekli olan ve bu nedenle değeri olan, dolayısı ile uygun şekilde **korunması** gereken bir varlıktır.

Bilgi Nedir?

Bilgi Güvenliği

Bilgi

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



Bilgi Güvenliği

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

- **Gizlilik**
- **Bütünlük**
- **Erişilebilirlik**

Bilgi Güvenliği

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

Bilgi güvenliği

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.

Neden Önemli?

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.

Neden Önemli?

İŞ SÜREKLİLİĞİ AKSAYABİLİR

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

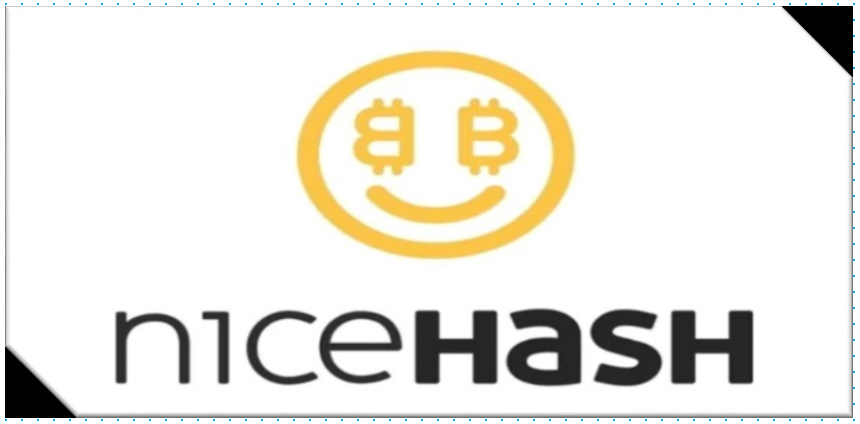
Sabit diskleri şifreleyerek kullanıcıdan şifreyi kaldırma karşılığı ücret talep etmektedir.

Neden Önemli?

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.



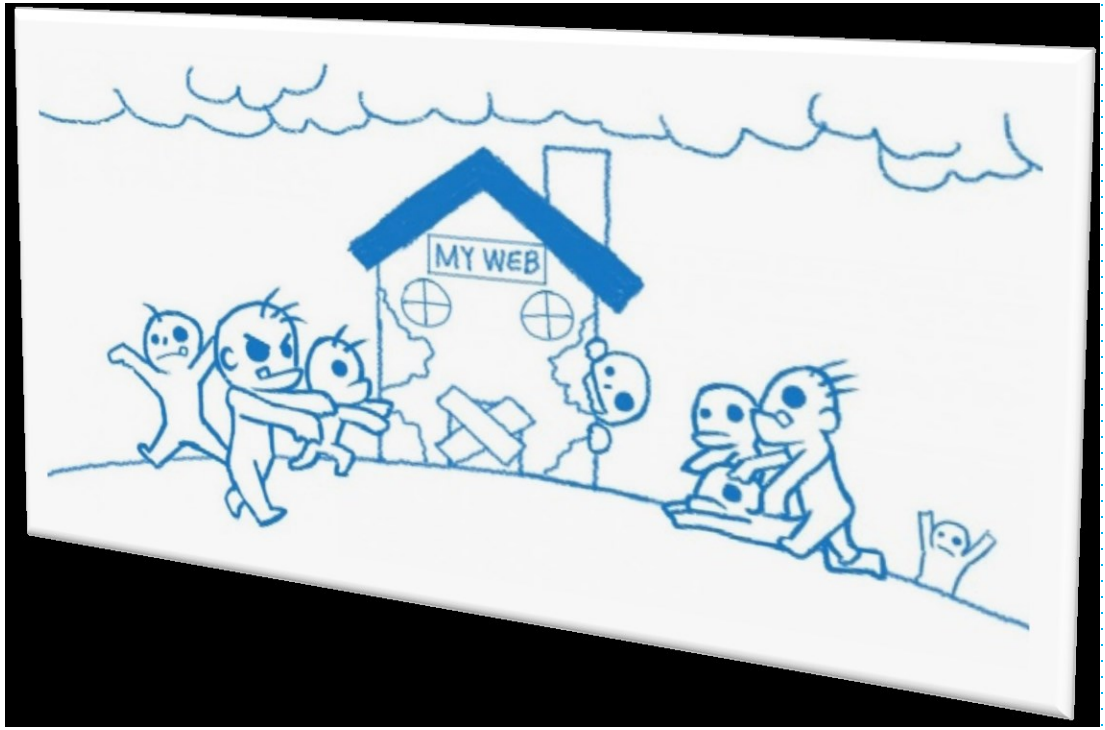
Neden Önemli?

YASAL YAPTIRIMLARLA KARŞILAŞILABİLİR

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

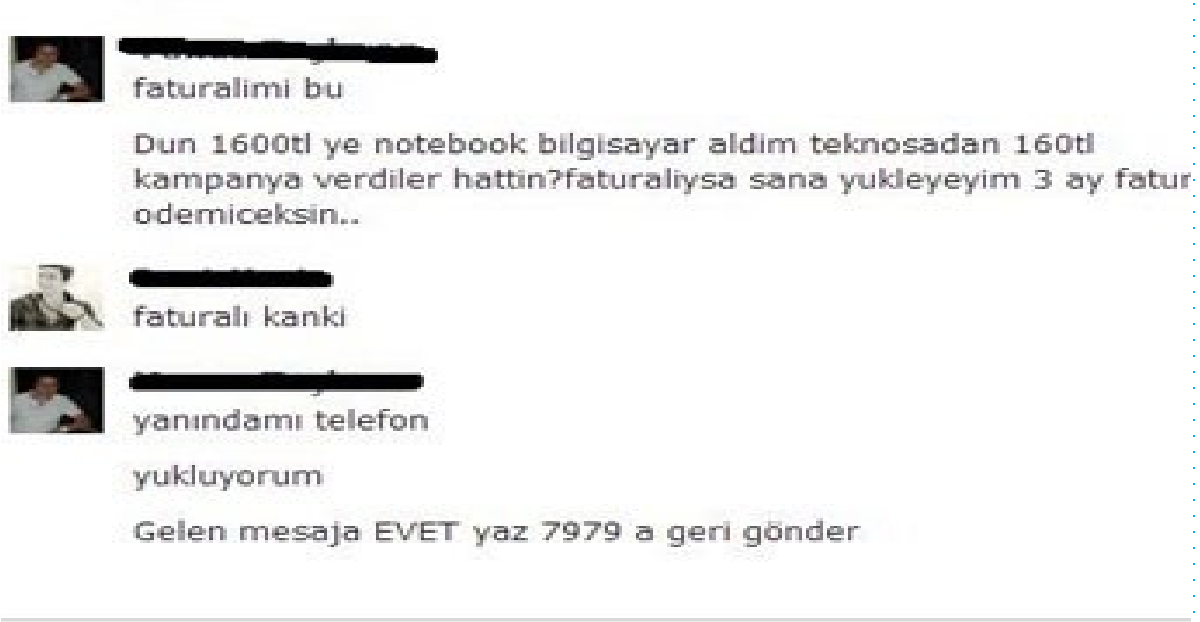
Bu nedenle yasal yaptırımlara maruz kalınabilir.

Neden Önemli?



ELEKTRONİK ORTAMDA SİZİN ADINIZA İŞLEM YAPILABİLİR

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



Neden Önemli?

Bilgisiz ve Bilinçsiz Kullanım

- Temizlik görevlisinin sunucunun fişini çekmesi
- Eğitilmemiş çalışanın veritabanını silmesi

Kötü Niyetli Hareketler

- İşten çıkarılan çalışanın, kuruma ait web sitesini değiştirmesi
- Bir çalışanın ağda özel yazılım ile ağ trafiğini okuması
- Bir yöneticinin, geliştirilen ürünün planını rakip kuruma satması

Tehditler nelerdir?

Hedefe Yönelmiş Saldırılar

- Bir saldırganın kurumun korunan bilgisini çalması
- Birçok saldırganın kurum web sunucusunu servis dışı bırakma saldırısı yapması

Tehditler nelerdir?

- 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 Bilincinin Önemi!

- Bir kullanıcının **güvenlik ihlali** tüm sistemi etkileyebilir.
- Teknik önlemler kullanıcı hatalarını önlemede yetersiz kalmaktadır.
- Kullanıcılar tarafından dikkat edilebilecek bazı kurallar sistemlerin güvenliğinin sağlanmasında kritik bir öneme sahiptir.

Kullanıcı Bilincinin Önemi!

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

- Bilgi Güvenliğini sağlamak;

TÜM ÇALIŞANLARIN SORUMLULUĞUNDADIR.

- Saldırganlar çoğunlukla **kullanıcı hatalarını** kullanmaktadırlar.

Kullanıcı Sorumlulukları

Bilgi Güvenliği

GÜVENLİK

Bilgi Güvenliği

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

- **Kritik bilgi içeren belgeler** yazıcılarda, fotokopi veya faks cihazlarında bırakılmamalıdır.
- Otomobil ile yapılan taşımalarda, bilgi içeren taşınabilir cihazlar bagajda taşınmalı, görünür şekilde araç içerisinde bırakılmamalıdır.
- Tüm **yedekleme ortamları fiziksel olarak güvenli** (nem, güneş, manyetik alan, toz, hırsızlık gibi tehditlerden korunabilecek) yerlerde saklanmalıdır.

FİZİKSEL GÜVENLİK

Bilgi Güvenliği

- Mesai sonlarında ve çalışma ortamından ayrıldığınızda masaüstü ve/veya dizüstü **bilgisayarlar kilitlenmeli**, gizli bilgi içeren evrak ve dijital medyalar saklanmalıdır.

- Toplantı sonrasında **tahtaya yazılanlar temizlenmeli** ve toplantı odasında evrak bırakılmamalıdır.

- Gizlilik derecesi yüksek bilgi ve belgelerin **kilitli dolap** ve çekmecelerde saklanması gerekmektedir.

FİZİKSEL GÜVENLİK

- Gizlilik derecesi yüksek bilgi içeren hiçbir varlık, **doğrudan çöpe atılmamalı**, kağıt imha makinası kullanılarak imha edilmelidir.

- Bilişim ve bilgi işlem sistemleri üzerinde depolanan bilginin imhası gerekli olduğunda, "**Güvenli Bilgi Silme**" amaçlı programlar kullanılmalıdır.

FİZİKSEL GÜVENLİK

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

FİZİKSEL GÜVENLİK

Etkin çözümler tercih edilmelidir. İşe yaramayacak önlemler alınmamalıdır.

FİZİKSEL GÜVENLİK

Bilgi Güvenliği

Kritik odalar adreslenmemelidir.

Fayda – Maliyet analizi yapılmalıdır. Güvenliği sağlamak varlığın kendi değerini geçmemelidir.

FİZİKSEL GÜVENLİK


" EN ETKİN KORUNMA YÖNTEMİ "
GLASBERGEN

Kişisel verilerin korunması için önce bilgisayarımıza yönelik tehditleri bilmeliyiz.

- Virüsler
- Casus Yazılımlar
- Solucanlar
- Reklam yazılımları
- Truva atları

Bilgisayar Güvenliği

VİRÜSLER

Bilgisayar virüsü, **kullanıcının izni ya da bilgisi dahilinde olmadan** bilgisayarın çalışma şeklini değiştiren ve kendini diğer dosyaların içerisinde gizlemeye çalışan aslında bir tür bilgisayar programıdır.

- Bilgisayarımıza bulaşarak **dosya ve programlarımıza** zarar verir.
- Virüsler bilgisayarınızda **bilgileri bozabilir** hatta silebilir.
- Bilgisayar virüsü pek çok zararlı yazılımdan çok daha tehlikelidir çünkü doğrudan **dosyalarınıza zarar verirler**.

Bilgisayar Güvenliği

TRUVA ATI (TROJAN)

Bilgisayar yazılım terimi olarak Truva atı zararlı kod içeren yazılım demektir. Terim klasik Truva atı efsanesinden türetilmiştir. Kullanıcıya **faydalı program gibi görünen** yazılım çalıştırıldığında bilgilerinize veya diğer programlarınıza **zarar** verir.

- Bilgisayarınızı uzakta erişime açabilirler,
- Elektronik posta gönderebilirler,
- Verilerinizi bozabilirler,
- Ağ geçitlerine saklanabilirler,
- Ağ dosya yükleme sistemine bulaşabilirler,
- Güvenlik yazılımınızı devre dışı bırakabilirler,
- Hizmet dışı saldırısı uygulayabilirler,
- İnternet erişiminize zarar verebilirler.

Bilgisayar Güvenliği

SOLUCAN (WORM)

Bilgisayar sistemleri üzerinde kendilerini otomatik olarak çoğaltan, sistemi çökertmeye veya yavaşlatmaya çalışan zararlı yazılım türüne solucan(**worm)** denir.

- Bu zararlı yazılım türü çalışmak için kullanıcı müdahalesi beklemez.
- Sistemlerde ki kaynak tüketimine ve bazı uygulamaların çalışmamasına neden olur.
- Arka kapı (**backdoor**) oluşturarak sisteme uzaktan bağlantı yapılmasını sağlar.

Bilgisayar Güvenliği

REKLAM YAZILIMI (ADWARE)

Adware (Reklam Yazılımı), bilgisayarınızda reklamlar görüntülemek, arama isteklerinizi reklam web sitelerine yeniden yönlendirmek ve özelleştirilmiş reklamların görüntülenmesi için ziyaret ettiğiniz web sitelerinin türleri gibi hakkınızdaki **pazarlama verilerini toplamak** amacıyla tasarlanmış programlara verilen addır.

Bilgisayar Güvenliği

CASUS YAZILIM (SPYWARE)

Spyware, bilgisayar kullanıcısının kendi rızası ve/veya bilgisi dışında veri toplayan casus yazılımlardır.

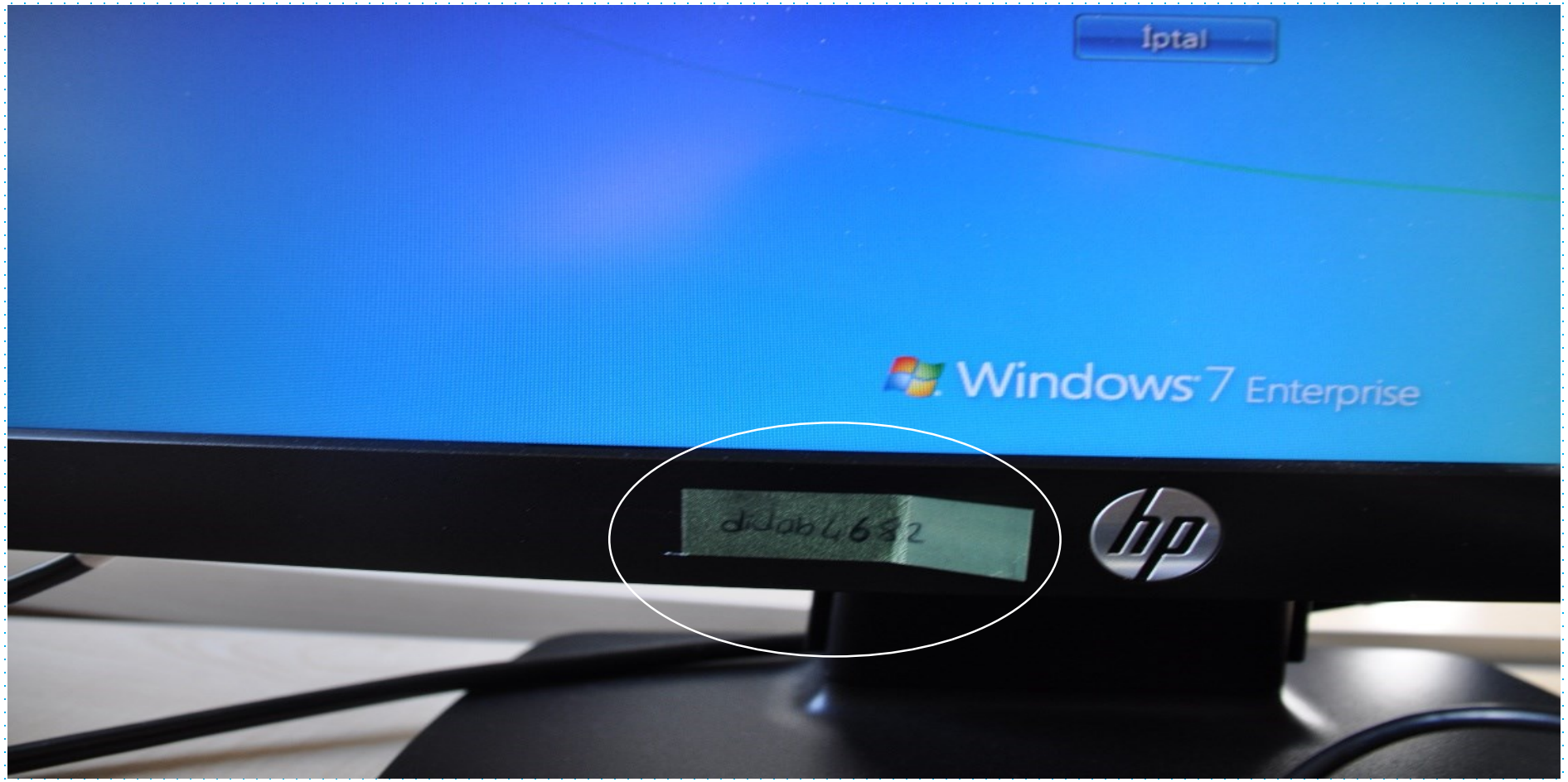
- Kullanıcının klavyede bastığı tuşları kaydetmek
- Görüntülediği web sayfalarının kaydını tutmak.
- Sabit diskindeki verileri taramak.
- İnternet'te yapılan aramaları izlemek.

Bilgisayar Güvenliği

Korunma Yolları

- Kullandığınız işletim sistemine ait **güncel**leştirmeleri ihmal etmeyin.
- **Ödül, hediye** vs. kazandığınızı belirten reklamlara aldanmayın, tıklamayın.
- Güvenmediğiniz bir bilgisayara USB bellek, hafıza kartı vs. takmayın.
- Kuruma ait **antivirüs** programı bilgisayarınızda yüklü olmalı ve **güncel** olmalı. Eğer güncelleme de sıkıntı çekiyorsanız yardım almalısınız.

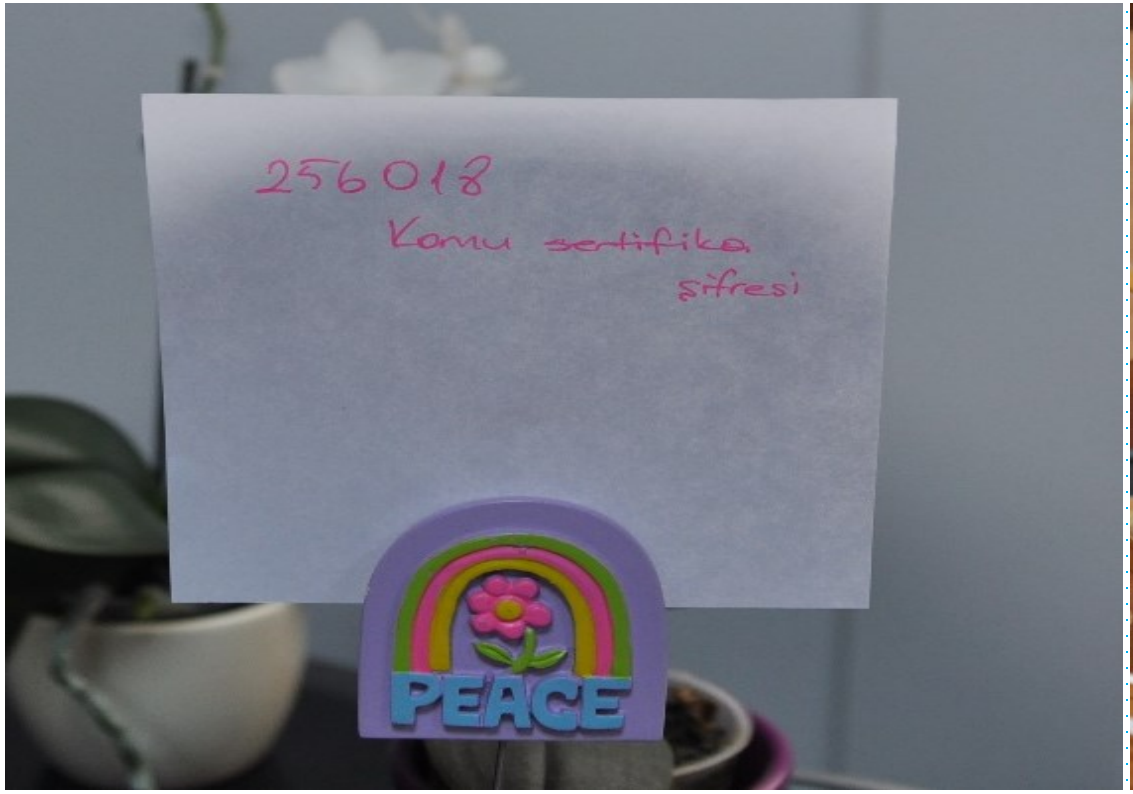
Bilgisayar Güvenliği



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

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, telatkaya, abcde, ahmet1979 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 kırılma süreleri

Uzunluk : 6 karakter

Küçük harf : 10 dk.

Küçük ve büyük harf :10 saat

Küçük harf + büyük harf + rakamlar + sembol : 18 gün

PAROLA GÜVENLİĞİ

Parola kırılma süreleri

Uzunluk : 8 karakter

Küçük harf : 4 gün

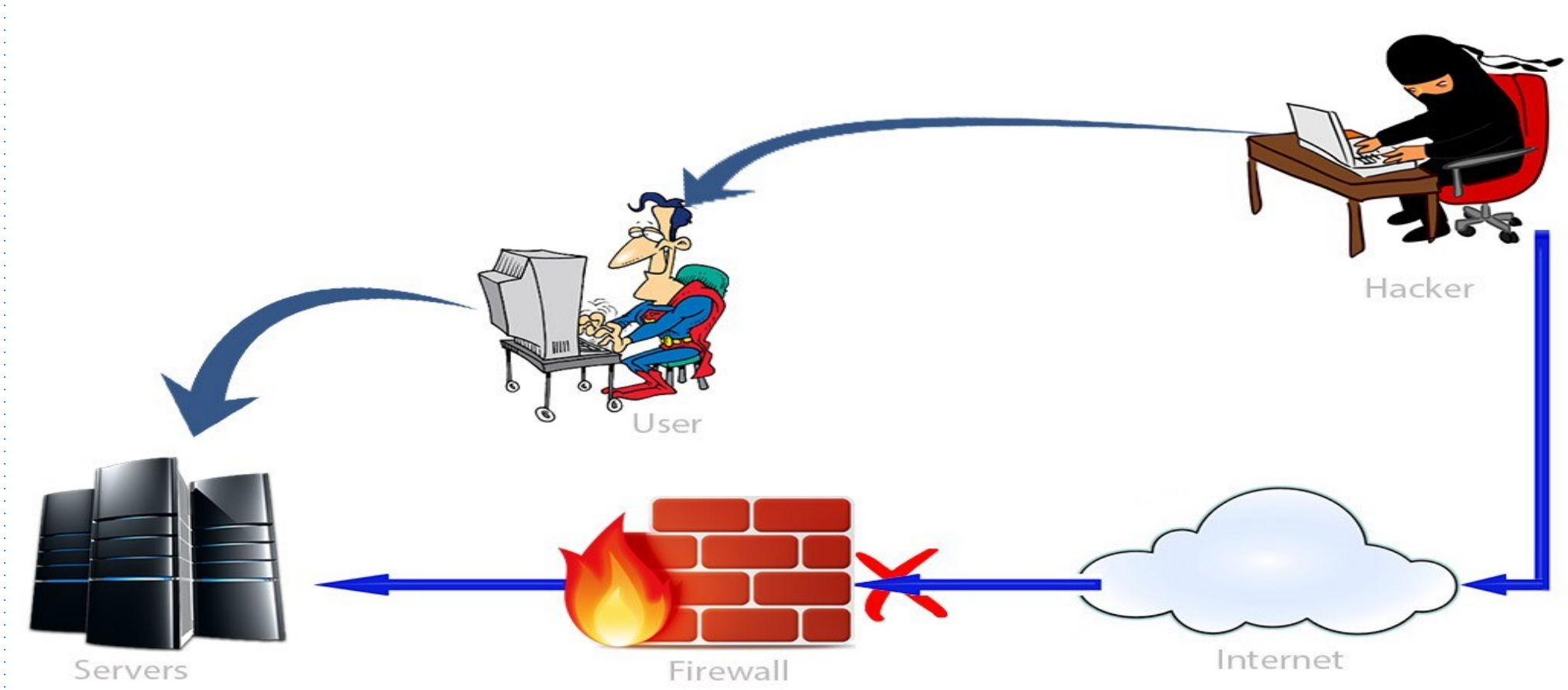
Küçük ve büyük harf : 3 yıl

Küçük harf + büyük harf + rakamlar + sembol : 463 yıl

PAROLA GÜVENLİĞİ

- 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.

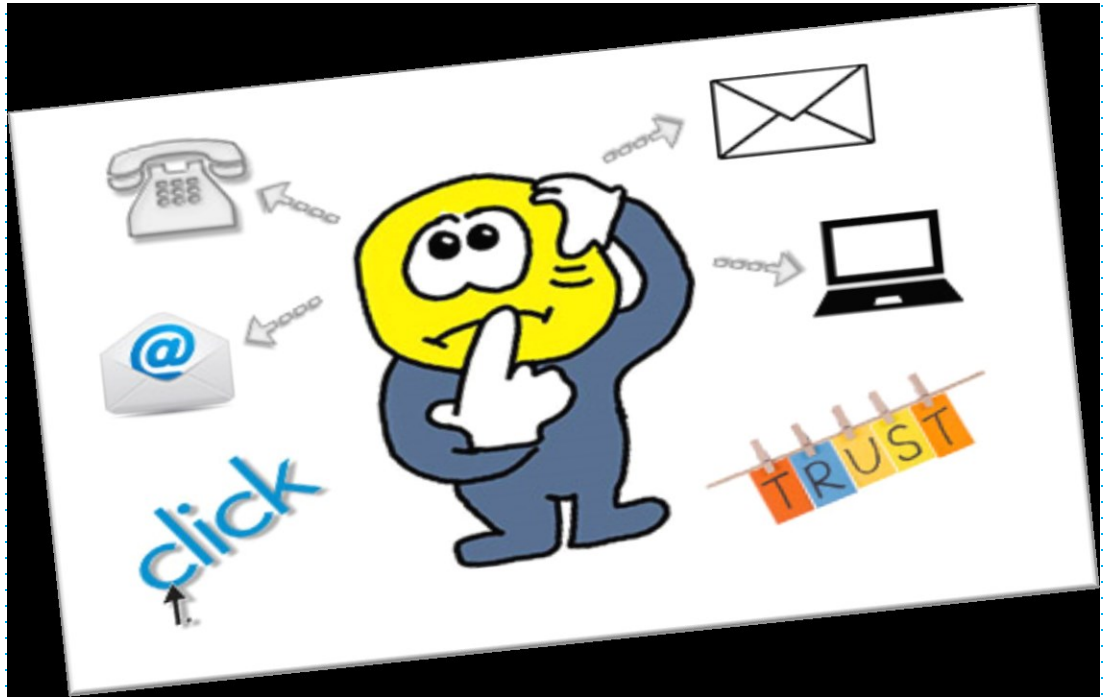
Sosyal Mühendislik



Sosyal Mühendislik

Sosyal Mühendislik Teknikleri

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

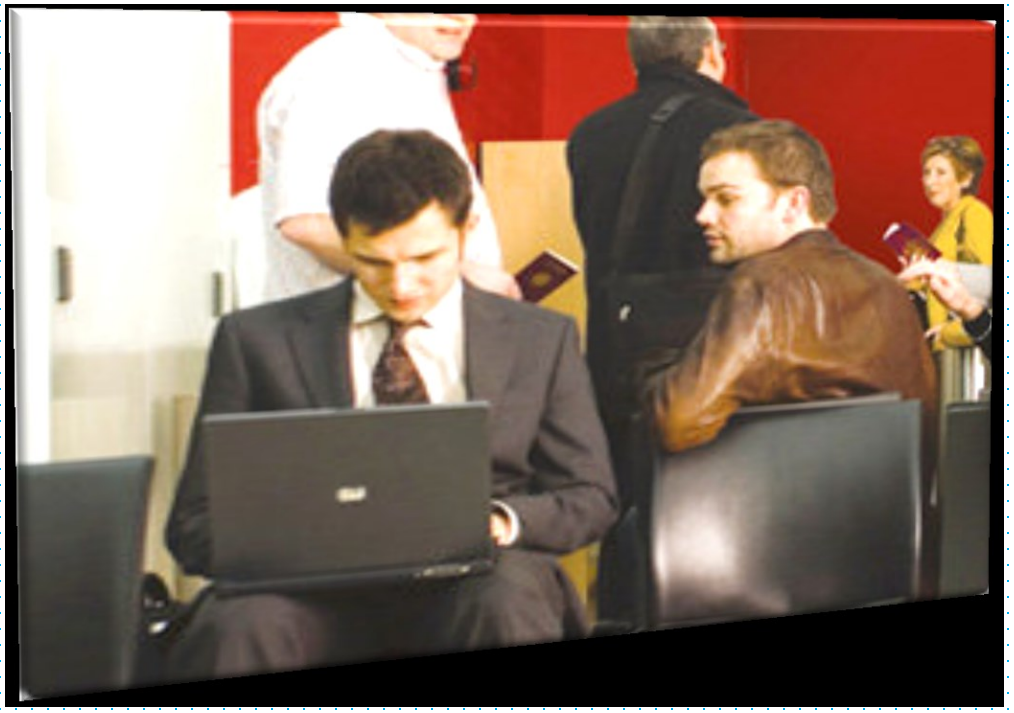


Sosyal Mühendislik

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.



Sosyal Mühendislik

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.

Sosyal Mühendislik

Truva Atı

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

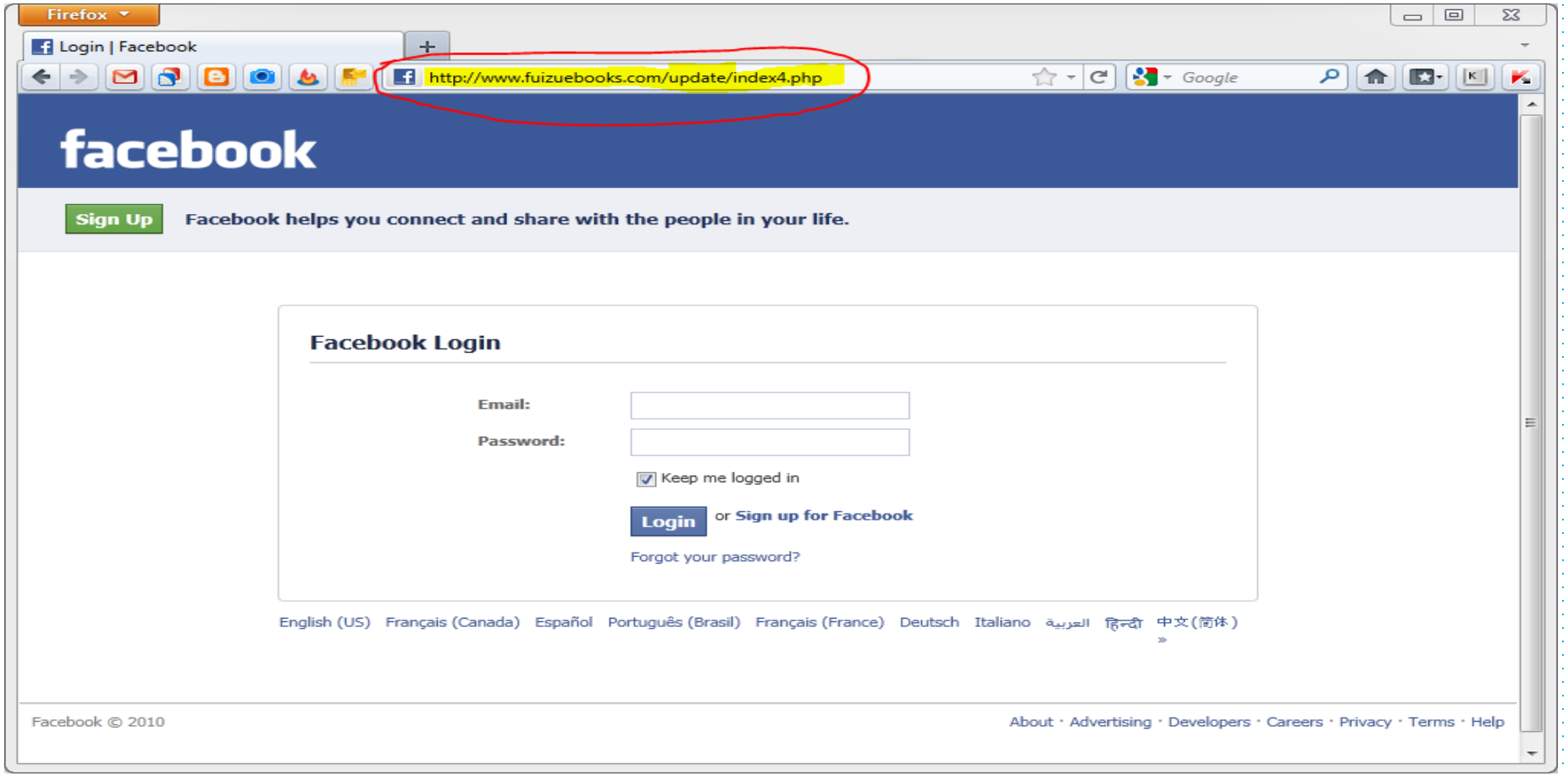
Sosyal Mühendislik

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 mühendislikte bu kişileri oltalamak için oluşturulacak senaryoya bilgi edinmek amacıyla kullanılmaktadır.

Sosyal Mühendislik



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.

Sosyal Mühendislik

Oltalama

İletişim yolları kullanılarak yapılan bir saldırı türüdür. Eposta, SMS ve diğer mesajlaşma yazılımları.

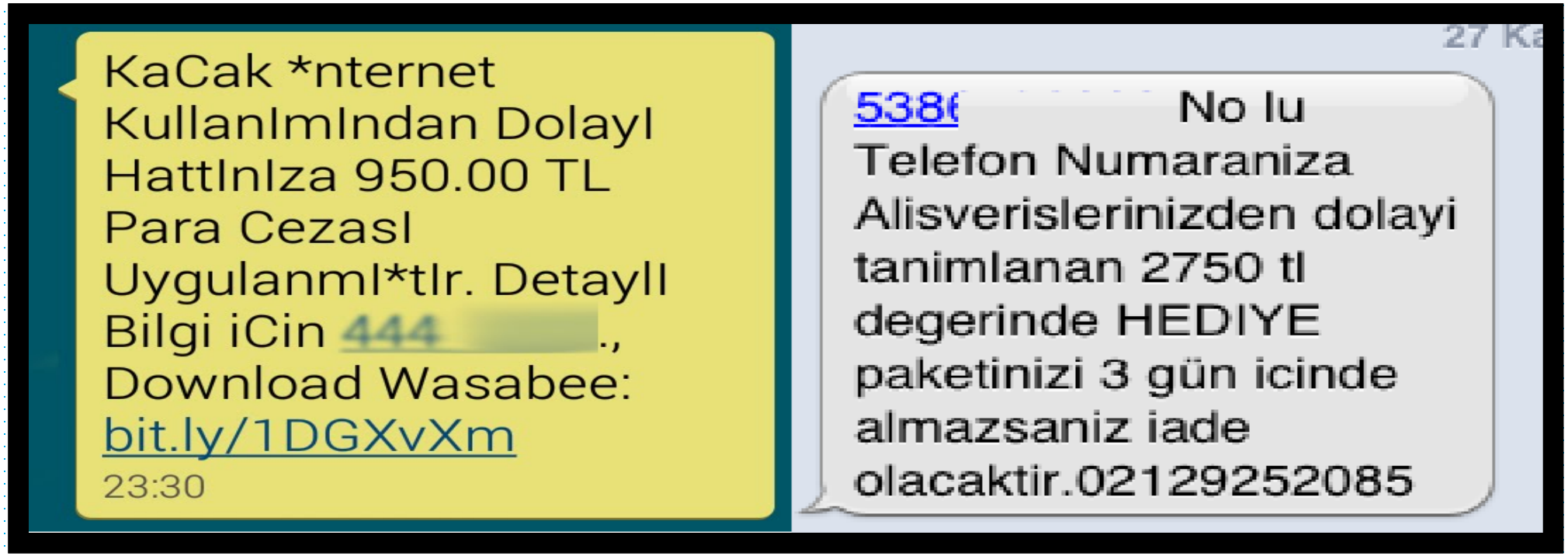
- **SMS** ile **ödül** kazandığınızı ve linke tıklayarak alabileceğinizi söyler.
- Mesajlaşma yazılımlarından arkadaşlarınıza bulaşan virüsler kendini taşımak için size sahte adres gönderir.
- En sık kullanılanı **Eposta** yoludur.

Sosyal Mühendislik

Oltalama

Sosyal Mühendislik

Oltalama



Sosyal Mühendislik

Tarih: 10 Kasım 2010, Çarşamba, 11:41
Gönderen: ahmetzen@golfgrup.com
Alıcı: sensin@postaci.com
Konu: yakın akraba

Sevgili Arkadaşım,
Ben Ali Gücen, Singapurda ve deneyimli bir muhasebe uzmanı olarak Bahraid Bankasında çalışmaktayım. Bu fırsatı size haber vermek ve sunmaktan büyük bir mutluluk duyuyorum; sizinle aynı soyadı taşıyan eski bir müşterimi geçtiğimiz pazar günü (07.11.2010) kalp krizi nedeniyle kaybettik. 26 Aralık 2004'te Sumatra yakınlarında gerçekleşen tsunami nedeniyle müşterim bütün yakınlarını, yani bütün varislerini kaybetmişti. Müşterimin hesabında bulunan 3.7 milyon dolar para için herhangi bir yakın akraba bulunamadı.

Müşterimin yaşayan hiçbir yakın akrabasının kalmadığından emin olduktan sonra, tek soyadı tutan kişi olarak, yakın akrabalık konusunda sizinle temasa geçmemin uygun olduğunda karar verdim. Ölen müşterimin tek varisi olarak kalan kaynağın size aktarılmasını planlayabilirim. Bu konuda herhangi bir çekinceniz olmaması için gerekli yasal bilgi ve belgelerin sizin adınıza düzenleneceğinizi belirtirim.

Mirasın sizin adınıza devriyle ilgili son tarihi kaçırmamak için ivedi olarak sizden bu konuda işbirliği ve anlayış konusundaki cevabınızı bekliyorum. Bu konuyla ilgileniyorsanız ve benimle işbirliği yapmayı kabul ediyorsanız, benimle hemen irtibata geçiniz. Size konuyla ilgili bilgi ve belgelerle birlikte, sizden ödeme için istenen dokümanlar konusunda en kısa zamanda iletişime geçeceğim. Bu süreçte hukuki işlemler için gerekli olan harcamaların %35'i sizin tarafınızdan, %65'i benim tarafımdan karşılanacaktır.

Saygılarımla,
Ahmet Akın,
mhyakin@safim.com

Sosyal Mühendislik

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.

Sosyal Mühendislik

Eposta Güvenliği

Elektronik postalar günümüzde bilgi hırsızlığı için kullanılan en etkin araçlardan birisidir.

Eposta Güvenliği

- **Kaynağı bilinmeyen** e-postalar kesinlikle açılmamalıdır.
- İçeriğinden **şüphe**lenilen e-postaların kaynağı doğrulanmalı (Örneğin; arkadaşınızdan gelen şüpheli bir e-posta, arkadaşınızı arayıp onaylatmadan açılmamalı!),
- E-posta **ekler**i çalıştırılmadan önce **antivirüs** taramasından geçirilmelidir.
- E-posta içerisinde bulunan şüpheli linklere tıklanmamalıdır.

Eposta Güvenliği

- İçeriğinden emin olunmayan veya insan zaaflarını kullanan e-postalar paylaşılmamalıdır

- Kurumsal e-posta hesapları kişisel amaçlar için kullanılmamalıdır (Facebook, Twitter, Alışveriş sitesi üyelikleri).

Eposta Güvenliği

Yedekleme

- Yedekleme işlemi; **kaybolma** veya **silinme** tehlikesi olan verilerin başka ortamda kopyalarını bulundurma işlemidir.

- USB Disk, CD, DVD ve benzeri araçlar kullanarak verilerinizin güvenliğini sağlayabilirsiniz.

Bilgi Güvenliğini sağlamak sadece bazı birimlerin sorumluluğunda değildir.

Bilgi Güvenliğini sağlamak

TÜM ÇALIŞANLARIN SORUMLULUĞUNDADIR

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.

Yasal Sorumluluklar

- Bir kullanıcı kendi kullandığı bilgisayar ile tüm ağa bağlı olduğundan kullanıcıya bulaşan bir tehdit tüm sisteme yayılabilir.
- E-posta ile gelen ".exe" uzantılı bir eklenti, resim dosyası ya da müzik dosyası beraberinde bir solucan ya da truva atı içerebilir.
- Kullanıcı ekteki dosyayı açtığında tüm sisteme zarar verebilecek bir yazılıma izin vermiş olabilir.

Yasal Sorumluluklar

- 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.

Bilgi Güvenliği İhlali

https://www.ihbarweb.org.tr/

İhbar

Kötücül Yazılım

- Bulaştığı bir bilgisayar sisteminde veya ağ üzerindeki diğer makinelerde zarara yol açmak veya çalışmalarını aksatmak amacıyla hazırlanmış yazılımların genel adıdır.

KÖTÜCÜL YAZILIM (Malware)

Virüsler

- Kullanıcı dosyalarını tehdit eden, bozabilen yani genel olarak bulaştığı işletim sisteminde zarara sebep olan yazılımlardır.

Worms(Solucan)

- Bilgisayarda bulunan ağ bağlantısı sayesinde herhangi bir dosyaya gizlenmek zorunda kalmayan virüs her bilgisayara ağ bağlantısı üzerinden çoğalabilir.

Backdoor (Arka kapı)

- Bir sisteme dışarıdan sızılabilmesi için o sistemde açık oluşturma işlemidir. Genellikle bazı portları açarak kendi üreticisinin ve/veya başka bir yazılımın sisteme sızmasını sağlayan yazılımlardır.

Browser Hijacking (Tarayıcı ele geçirme)

- Bazı web siteleri tarafından, sayfalarının ziyaret sayısını arttırmak, kendi web sitelerindeki reklamların yüksek görüntülenme rakamlarına ulaşmasını sağlamak amacıyla web tarayıcınıza yerleştirilen, başlangıç sayfalarını ve arama sayfalarını değiştirebilen küçük bir program ya da registry ayarıdır. Eğer internet arama sayfalarınız ya da ana sayfanız sizin istemediğiniz bir şekilde değişiyorsa muhtemelen bilgisayarınızda böyle bir casus program yer edinmiştir.

Spyware (Casus)

- internette dolaşırken, ziyaret edilen siteleri, bu sitelerin içeriklerini sık kullanılan programları internet üzerinden üreticisine gönderir. internette dolaşırken tuzak pencerelere tıklandığında bilgisayara kurulur.

PHISHING

- "Password" (Şifre) ve "Fishing" (Balık avlamak) sözcüklerinin birleştirilmesiyle oluşturulan Türkçe'ye yemleme (oltalama) olarak çevrilmiş bir saldırı çeşididir. Phishing saldırıları son zamanların en gözde saldırı çeşidi olarak karşımıza çıkmaktadır. Yemleme yöntemi kullanılarak bilgisayar kullanıcıları her yıl milyarlarca dolar zarara uğratılmaktadır.

- Yemleme genelde bir kişinin şifresini veya kredi kartı ayrıntılarını öğrenmek amacıyla kullanılır. Bir banka veya resmi bir kurumdan geliyormuş gibi hazırlanan e-posta yardımıyla bilgisayar kullanıcıları sahta sitelere yönlendirilir. Phishing saldırıları için 'Bankalar, Sosyal Paylaşım Siteleri, Mail Servisleri, Online Oyunlar vb. sahte web sayfaları hazırlanmaktır. Burada bilgisayar kullanıcısında özlük bilgileri, kart numarası, şifresi vb. istenir. E-posta ve sahte sitedeki talepleri dikkate alan kullanıcıların bilgileri çalınır.

SNIFFER(KOKLAYICI)

- Sniffer adı verilen yazılımlarla bir ağ üzerindeki veri paketini yakalamak ve içeriğini okumaktır. Sniffing yöntemi çoğunlukla ağ uzmanları tarafından ağda bir sorun olup olmadığını kontrol etmek yada verilerin şifreli olarak iletildiğini kontrol etmek amacıyla kullanılır. Kötü niyetli kişiler, cracker ve black hat hacker'lar ise bu yöntemi şifreleri veya ağ yetkisini ele geçirmek için kullanabilirler.

ADWARE

- İngilizce açılımı ile **advertising-supported software** yani reklam destekli yazılım, yüklenildiği bilgisayara yüklenme işleminden sonra program kullanımdayken otomatik olarak çalışan, gösteren ve indirme yapan bir yazılım paketidir. Adware'lerin bazı tipleri spyware statüsündedir ve kişisel bilgilere gizlice ulaşılmasında kullanılırlar.

Bulaşma Yöntemleri

- Bazı masa üstü programlar ile beraber.
- Faydalı bir yazılım kurulumu sırasında.
- Lisans sözleşmeleri esnasında.
- Mail eklentileri ile.
- Tarayıcıların eksiklikleri
- Bilinçsiz kullanıcıları aldatarak.

Belirtileri

- Bilgisayarın performansı düşme durumunda,
- Web tarayıcı tuhaf siteleri açıyorsa,
- Farklı arama motoruna yönlendiriyorsa,
- Sık kullanılanlara farklı siteler eklenmişse,
- Home sayfası değişmişse,
- Tarayıcıda farklı seçenekler mevcutsa,
- İnternet yokken bile reklamlar çıkıyorsa
- Hata mesajları geliyorsa...

Korunma Yöntemleri

- İşletim sistemi güncellemesi
- Anti virüs programları
- Güvenlik duvarı
- Dayanıklı şifreler
- Orijinal programlar
- Bilinmeyen programları barındırmama...

SUÇ NEDİR?

- BAŞKA İNSANLARIN VEYA TÜZEL KİŞİLİKLERİN HAKLARINA TECAVÜZ ETMEK VEYA YANLIŞ YA DA ZARARLI OLDUĞU İÇİN YASAKLANAN VE BAZI DURUMLARDA CEZALANDIRILAN DAVRANIŞ OLARAK TANIMLANABİLİR.

BİLİŞİM

- İNSANLARIN TEKNİK, EKONOMİK VE TOPLUMSAL İLETİŞİMDE KULLANDIĞI VE BİLİMİN DAYANAĞI OLAN BİLGİNİN, DÜZENLİ VE AKLA UYGUN BİR BİÇİMDE, ÖZELLİKLE BİLGİSAYARLAR VE BENZERİ ELEKTRONİK AYGITLAR ARACILIĞIYLA İŞLENMESİ BİLİMİ.

BİLİŞİM SUÇU

- BİLİŞİM ALANINDA KULLANILAN ARAÇLARDAN YARARLANILARAK İŞLENİLEN SUÇLAR, BİLİŞİM SUÇU OLARAK TANIMLANMAKTADIR.

- BİLİŞİM SUÇLARI TCK'DE BİLİŞİM SİSTEMLERİ KULLANILARAK İŞLENEN SUÇLAR OLARAK TANIMLANMAKTADIR.

- BİLGİNİN, PROGRAMLARIN, SERVİSLERİN, EKİPMANLARIN VEYA HABERLEŞME AĞLARININ YIKIMI, HIRSIZLIĞI, YASADIŞI KULLANIMI, DEĞİŞTİRİLMESİ VEYA KOPYALANMASI DA, BİLİŞİM SUÇLARI OLARAK TANIMLANMAKTADIR.

NEDEN BİLİŞİM SUÇU İŞLENİR?

- MADDİ KAZANÇ ELDE ETMEK,
- KİŞİLERİN İTİBARINI SARSMAK,
- İNTİKAM ALMAK,
- SOSYAL HAYATTA İNSANLARA AKTARAMADIĞINI SANAL ORTAMDA GERÇEKLEŞTİRMEK,
- KARALAMAK VEYA YAKALANMA İHTİMALİNİN ZOR OLDUĞUNU DÜŞÜNEREK ZEVK AMAÇLI SALDIRI YAPMAK…

- BİLGİNİN, PROGRAMLARIN, SERVİSLERİN, EKİPMANLARIN VEYA HABERLEŞME AĞLARININ YIKIMI, HIRSIZLIĞI, YASADIŞI KULLANIMI, DEĞİŞTİRİLMESİ VEYA KOPYALANMASI DA, BİLİŞİM SUÇLARI OLARAK TANIMLANMAKTADIR.

ÖRNEK BİLİŞİM SUÇLARI

- KART KOPYALAMA
- E-TİCARET DOLANDIRICILIĞI
- KAMU KURUMLARINDA KEYFİ DAVRANIŞLAR…
- SAHTE MAİLLER İLE TEHDİT & ŞANTAJ
- KİŞİSEL BİLGİLERİN İHLALİ

Adli Bilişim Nedir

- Elektromanyetik ortamlarda muhafaza edilen veya bu ortamlarca iletilen ses, görüntü, veri, bilgi veya bunların birleşiminden oluşan her türlü bilişim nesnesinin, mahkemede sayısal delil niteliği taşıyacak şekilde tanımlanması, elde edilmesi, saklanması, incelenmesi ve mahkemeye sunulması çalışmaları bütünüdür.

Adli Bilişim Alanları

- Veri kurtarma
- Veri imha etme
- Veri saklama
- Veri dönüştürme
- Şifreleme(Kriptografi)
- Şifre çözme
- Gizlenmiş dosya bulma.

Adli Bilişim Uzmanı

- Bilişim sistemleri konusunda ileri derecede bilgi sahibi olan kimsedir.
- Adli bilişim uzmanı kabul edilmek için birtakım sertifika programları mevcuttur. Bu programlardan birine devam ederek sertifika almak ve adli bilişim uzmanı sıfatına sahip olmak mümkündür.

2025-2026

ÇAĞ ÜNİVERSİTESİ
ÇAĞ UNIVERSITY

Teşekkürler

Soru - Cevap

Dr. Öğr. Üyesi Taylan Tutkunca

MESLEK YÜKSEKOKULU