



NEVŞEHİR HACI BEKTAŞ VELİ ÜNİVERSİTESİ

BİLGİ GÜVENLİĞİ FARKINDALIK EĞİTİMİ

Öğr. Gör. Kürşat İLHAN

- Bu eğitimin amacı, **bilgi güvenliğine** yönelik yaygın tehditler ile bu tehditlere karşı alınabilecek önlemler hakkında bilgi vermek ve bu konuda belirli bir **farkındalık** oluşturmaktır.
- Bilgi güvenlik yapısında **en zayıf halka** olarak anılan **son kullanıcıların** oluşturduğu tehdit tamamen ortadan kaldırılamasa da iyi planlanmış ve **güvenlik bilincini** geliştirmeyi amaçlayan bir program, riskleri azaltmaya yardımcı olur. Bu eğitimin amacı, **etkili bir güvenlik stratejisi** uygulayarak farkındalığı en üst seviyeye taşıyabilmektir.

Eğitimin Amacı



- 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



İÇERİK

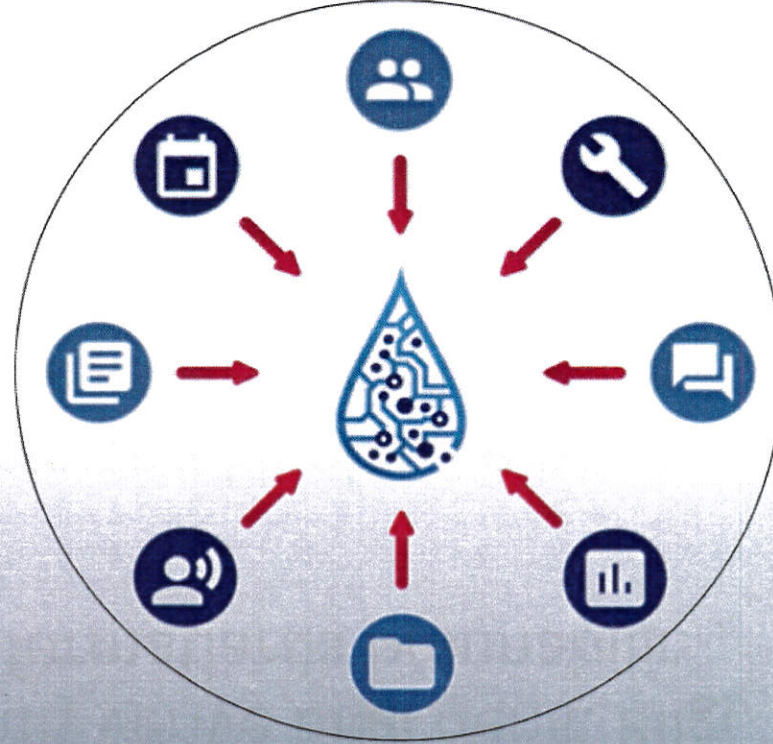
- Güvenli olmayan yazılımlar nelerdir ve korunmak için neler yapılmalıdır?
- E-posta güvenliği
- Yedekleme
- Bilgi sınıflandırma ve etiketleme
- Sosyal mühendislik yöntemleri ve dikkat edilmesi gerekenler
- Güvenli internet
- Yasal sorumluluklar
- Bilgi güvenliği ihlal olayları
- Sistemin devamlılığının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



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



Bilgi

Kurumun en değerli varlığı olan Bilgi'nin kaybolmasını, zarara uğramasını, yok olmasını, yetkisiz ve **kötü niyetli** kişilerin **eline geçmesini** 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 geçirilerek 3 milyar kullanıcının verileri çalınmıştı. Yahoo gelmiş geçmiş en büyük veri hırsızlığına maruz kaldı.

The image shows the classic Yahoo! logo in a purple serif font, with the exclamation mark being a larger, stylized font.

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

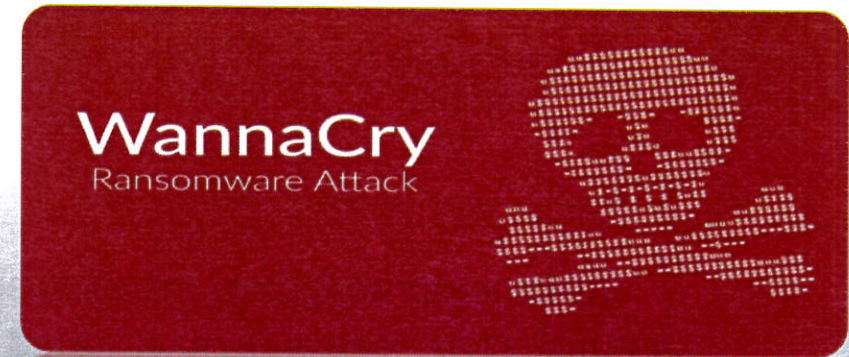


Neden Önemli?

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.

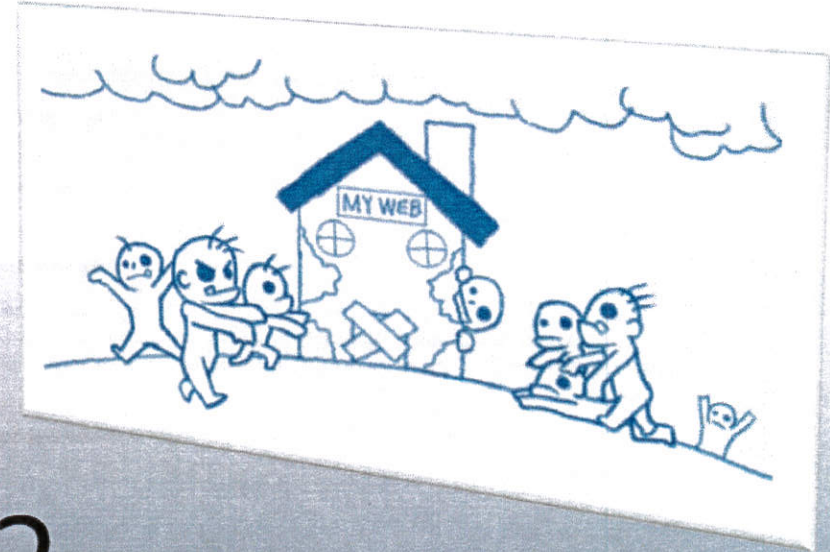


Neden Önemli?

YASAL YAPTIRIMLARLA KARŞILAŞILABİLİR

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

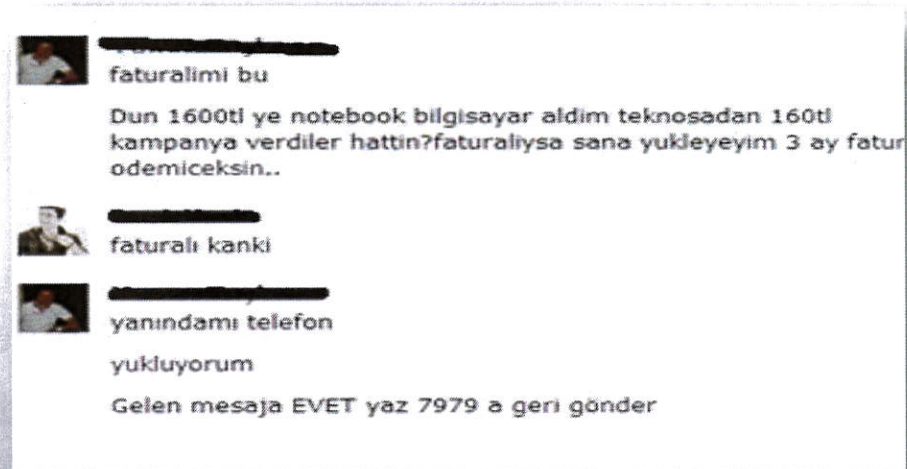
Bu nedenle yasal yaptırımlara maruz kalınabilir.



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?

SİBER SAVAŞLAR



Neden Önemli?

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.

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 bilincidir**.
- 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

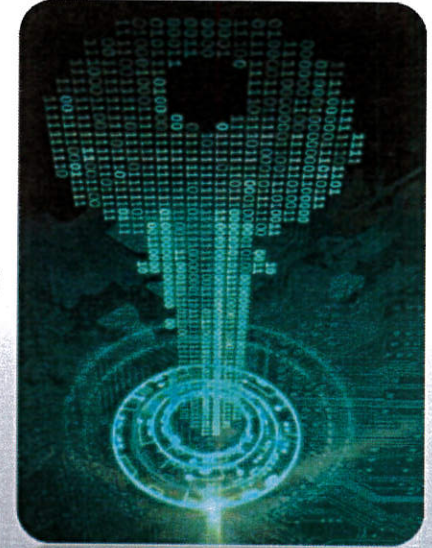


GÜVENLİK

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

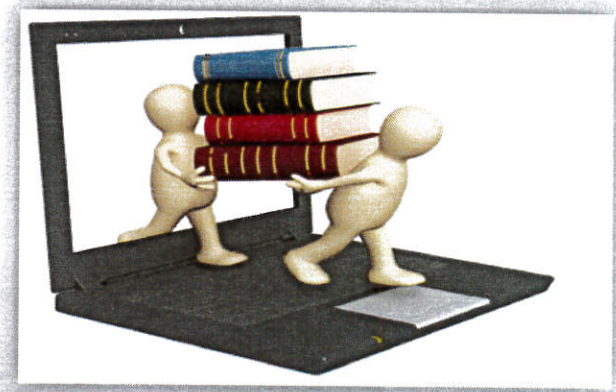


- **Kritik bilgi içeren belgeler** yazıcılarda, fotokopi veya faks cihazlarında bırakılmamalıdır.
- Otomobil ile yapılan taşımalarda, bilgi içeren taşınabilir cihazlar bagajda taşınmalı, görünür şekilde araç içerisinde bırakılmamalıdır.
- Tüm **yedekleme ortamları fiziksel olarak güvenli** (nem, güneş,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



FİZİKSEL GÜVENLİK

- 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 çekmecerde 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

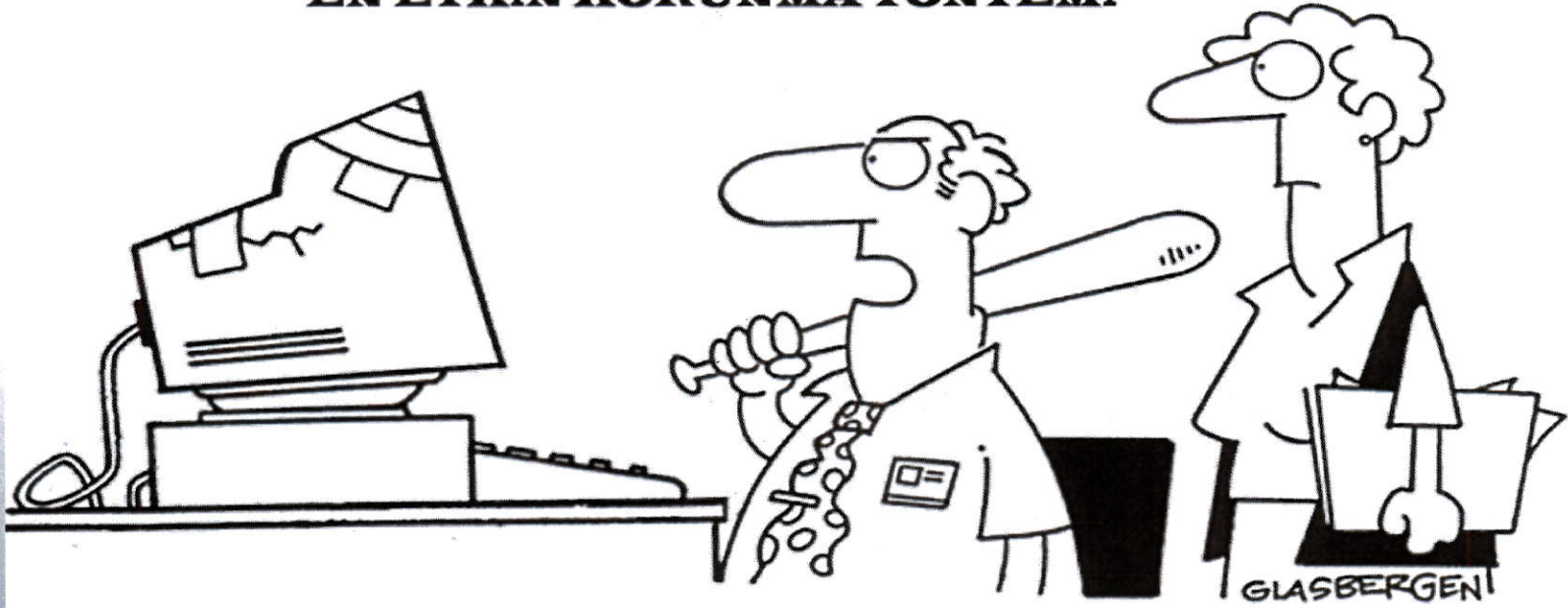
Kritik odalar adreslenmemelidir.

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



FİZİKSEL GÜVENLİK

“ EN ETKİN KORUNMA YÖNTEMİ ”



**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.

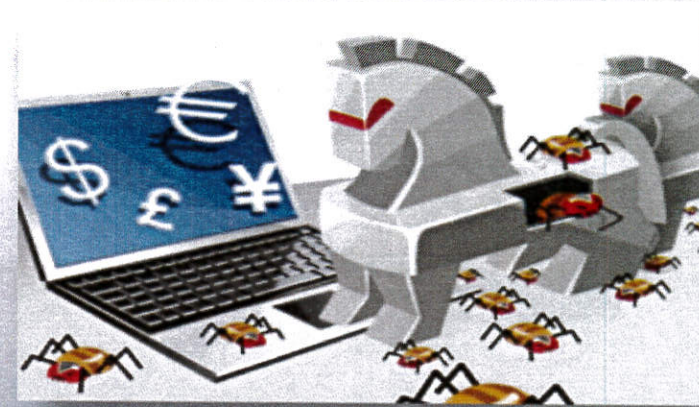


Bilgisayar Güvenliği

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 diskteki verileri taramak.
- İnternet'te yapılan aramaları izlemek.



Bilgisayar Güvenliği

Korunma Yolları

- Kullandığınız işletim sistemine ait **güncelleştirmeleri** 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.

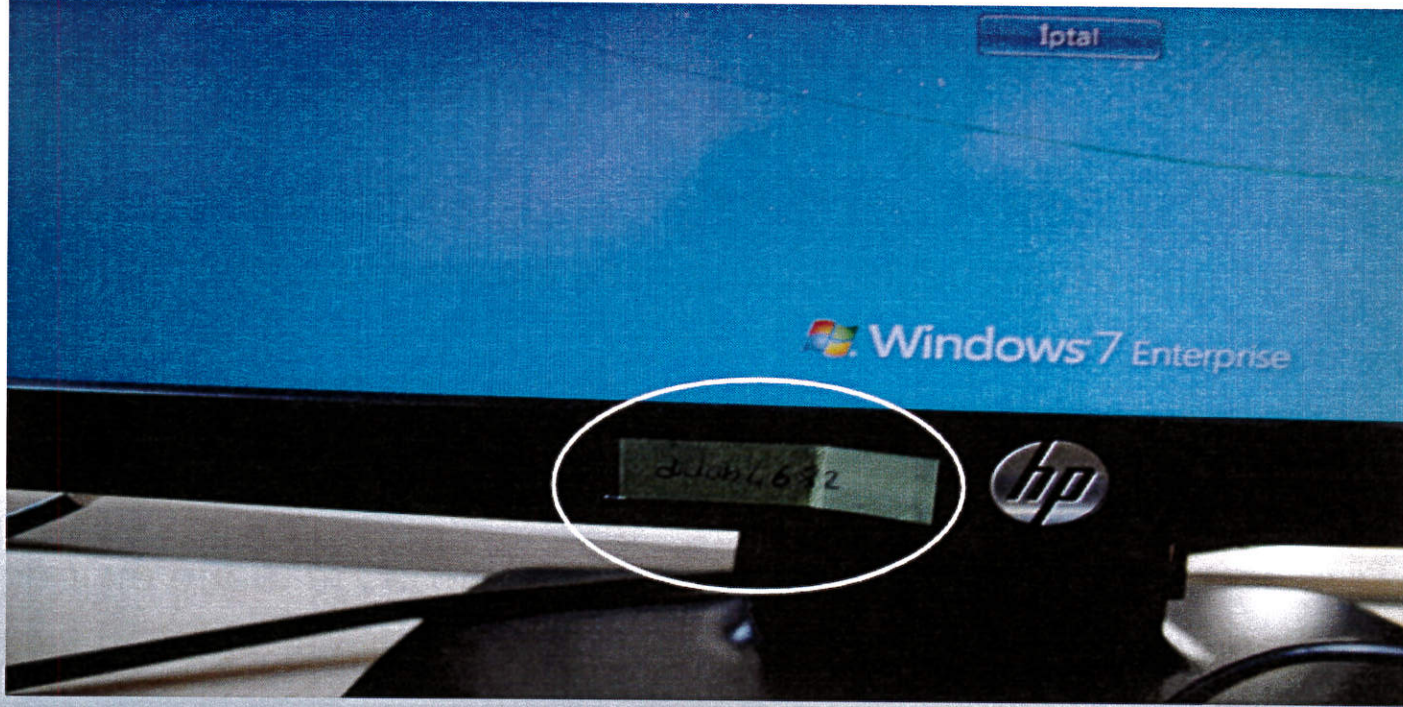


Bilgisayar Güvenliği

<https://www.youtube.com/watch?v=t35BkYWGWes>

<https://www.youtube.com/watch?v=0mqxeD95J-s>

Videolar

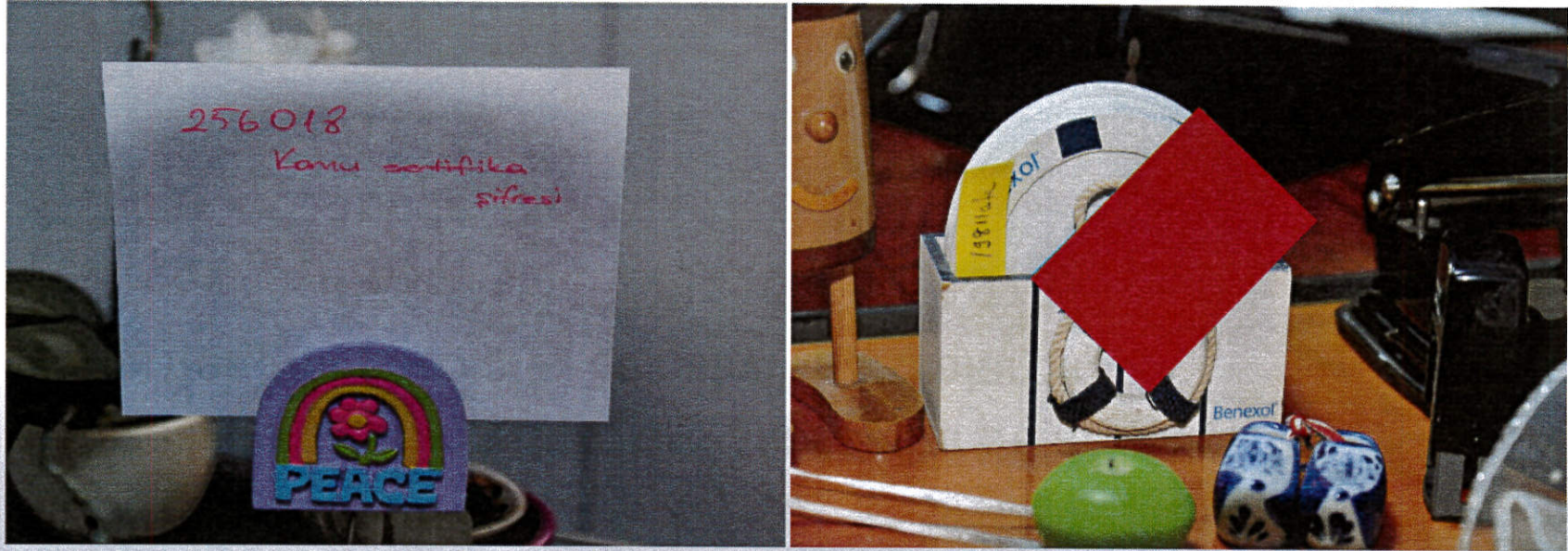


PAROLA GÜVENLİĞİ

- 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

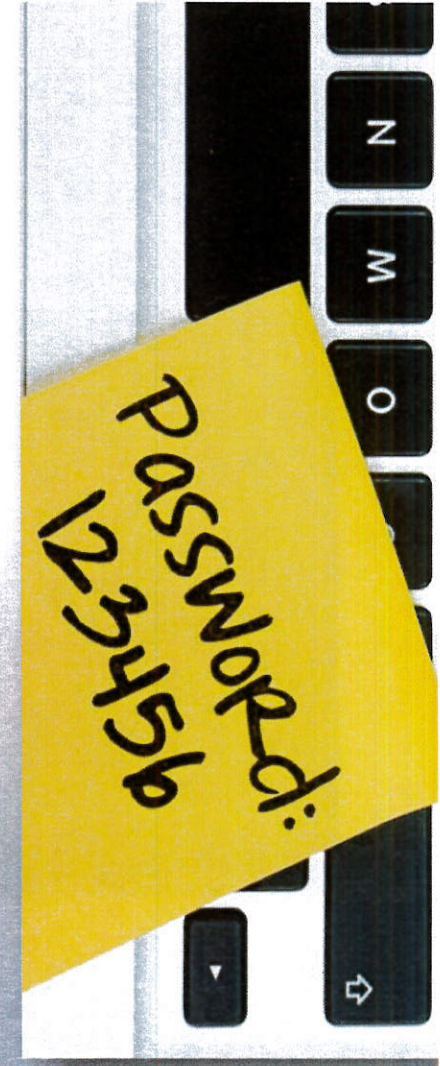




PAROLA GÜVENLİĞİ

- 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.

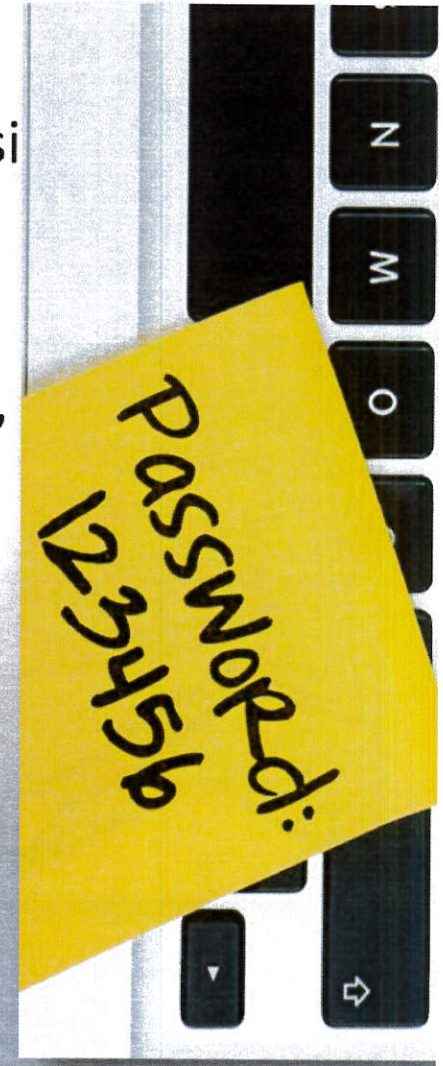
PAROLA GÜVENLİĞİ



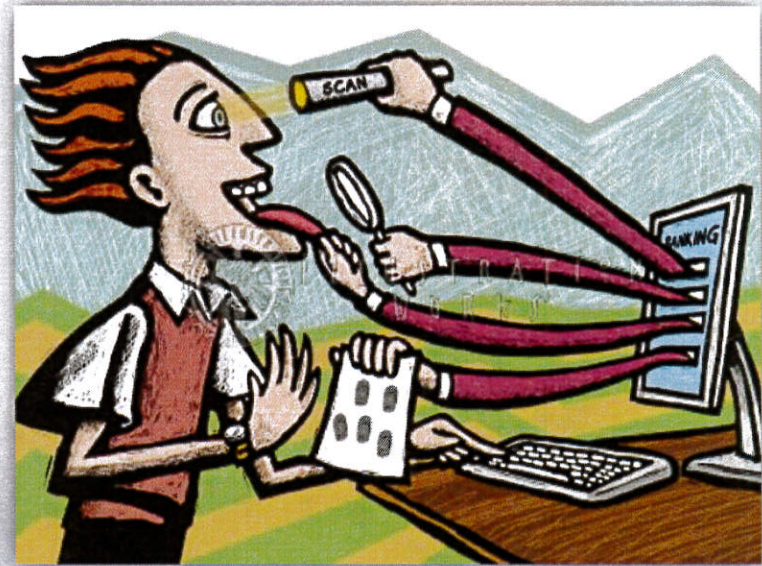
Oluşturulan bir parolanın "**güçlü**" kabul edilebilmesi için aşağıdaki özellikleri göstermelidir.

- **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 GÜVENLİĞİ

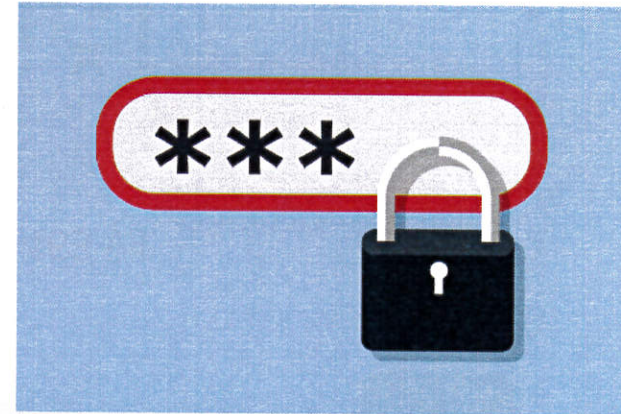
Parola kırılma süreleri

Uzunluk : 6 karakter

Küçük harf : 10 dk.

Küçük ve büyük harf : 10 saat

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



PAROLA GÜVENLİĞİ

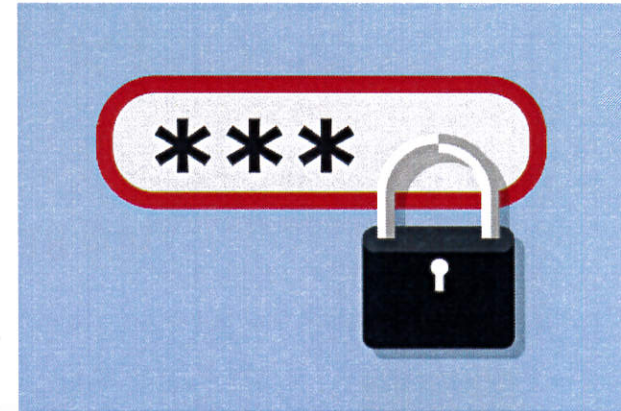
Parola kırılma süreleri

Uzunluk : 8 karakter

Küçük harf : 4 gün

Küçük ve büyük harf : 3 yıl

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

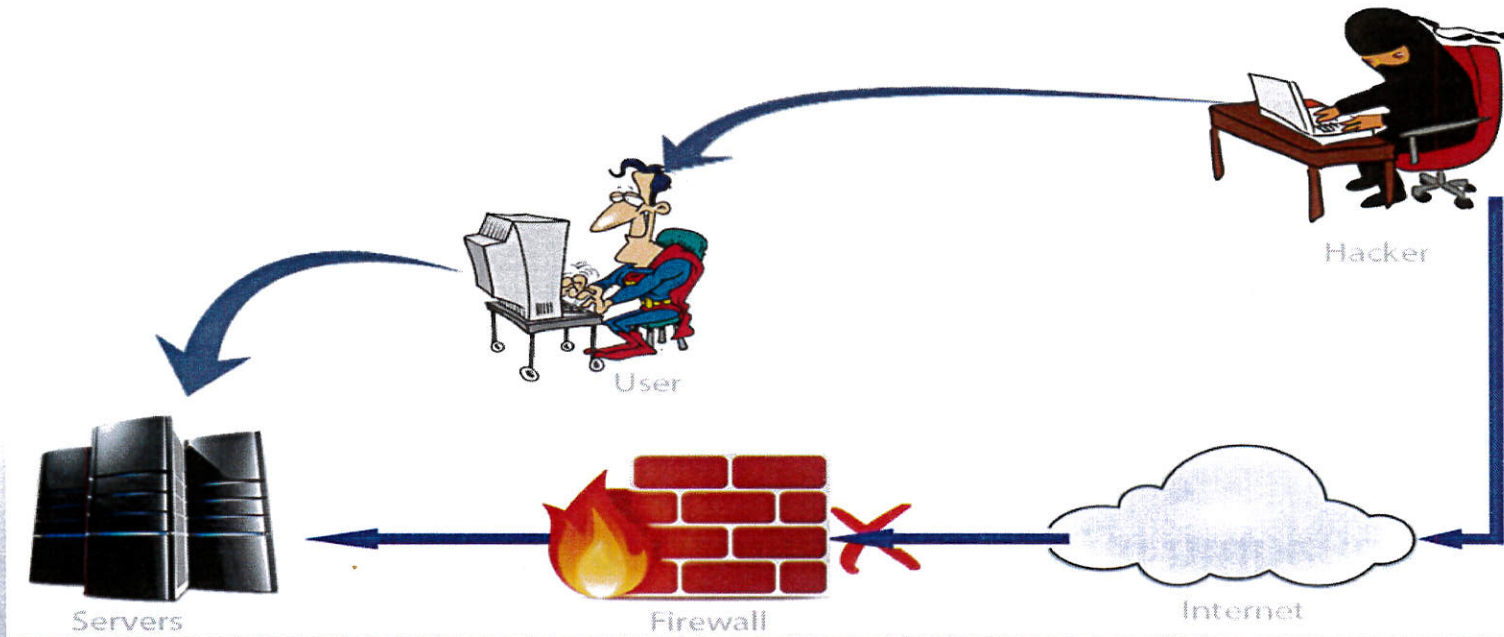


PAROLA GÜVENLİĞİ

- 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.



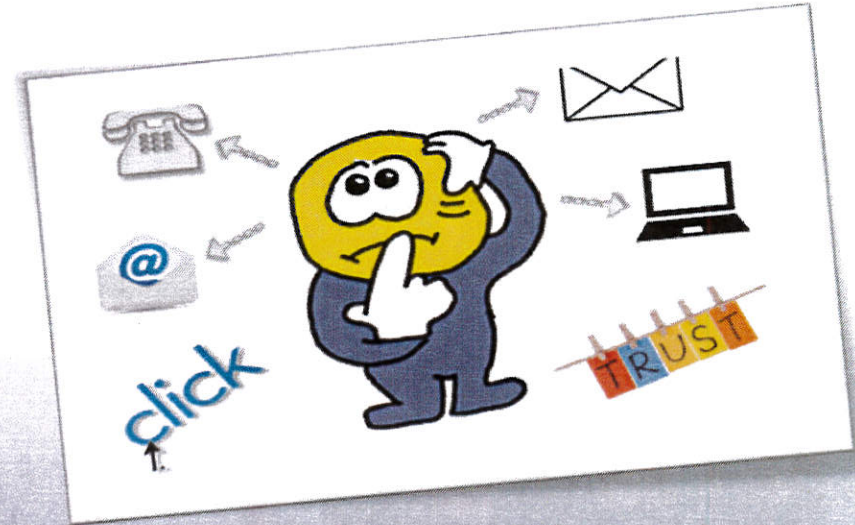
Sosyal Mühendislik



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.

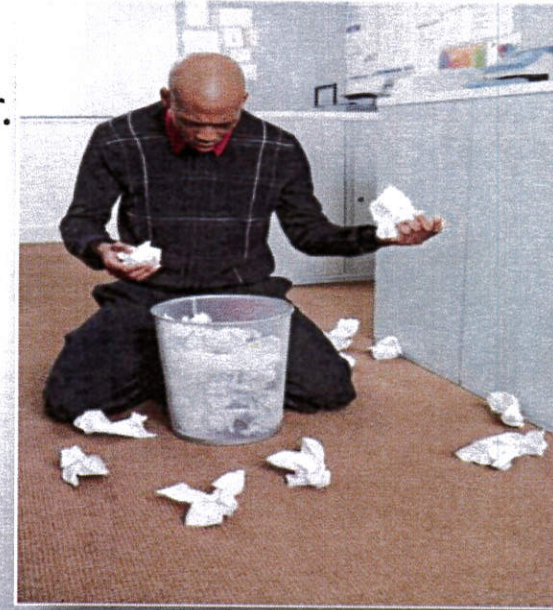


Sosyal Mühendislik

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

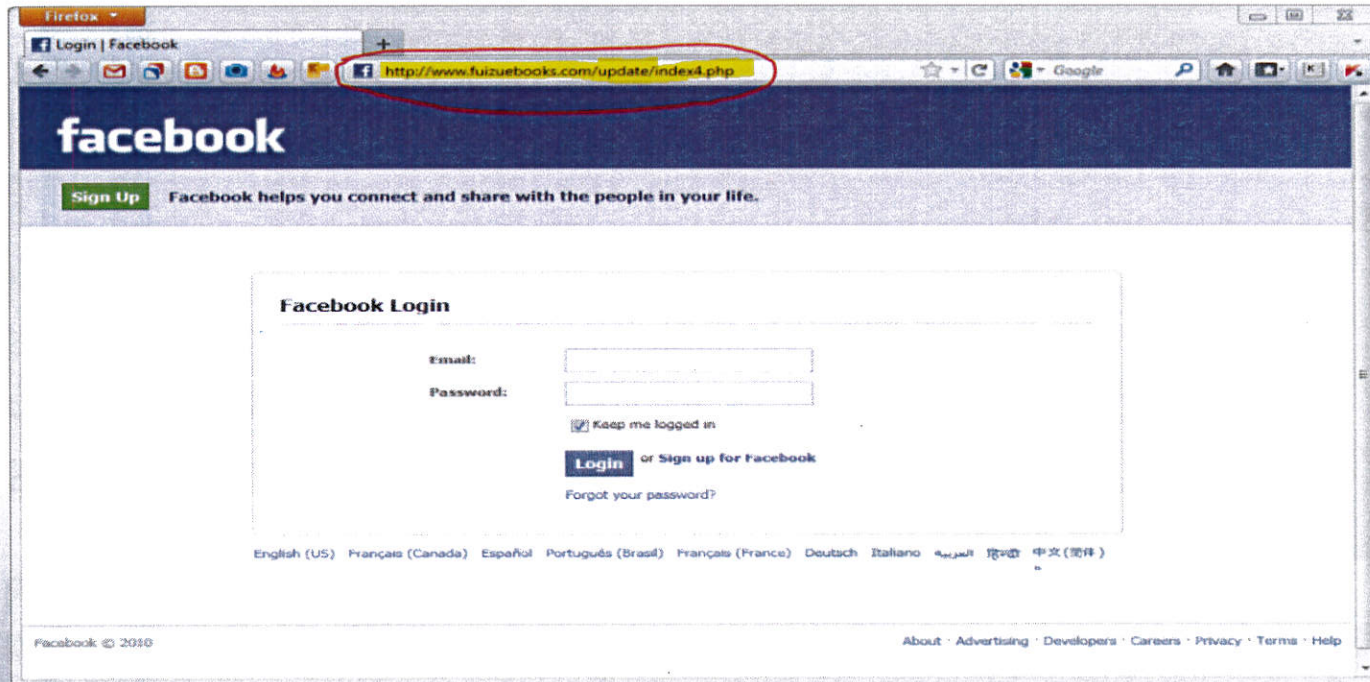


Rol Yapma

- Dolandırıcılıkta günümüzün en yaygın kullanım şeklidir. Telefonla arayarak kendisinin **bankadan** 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.

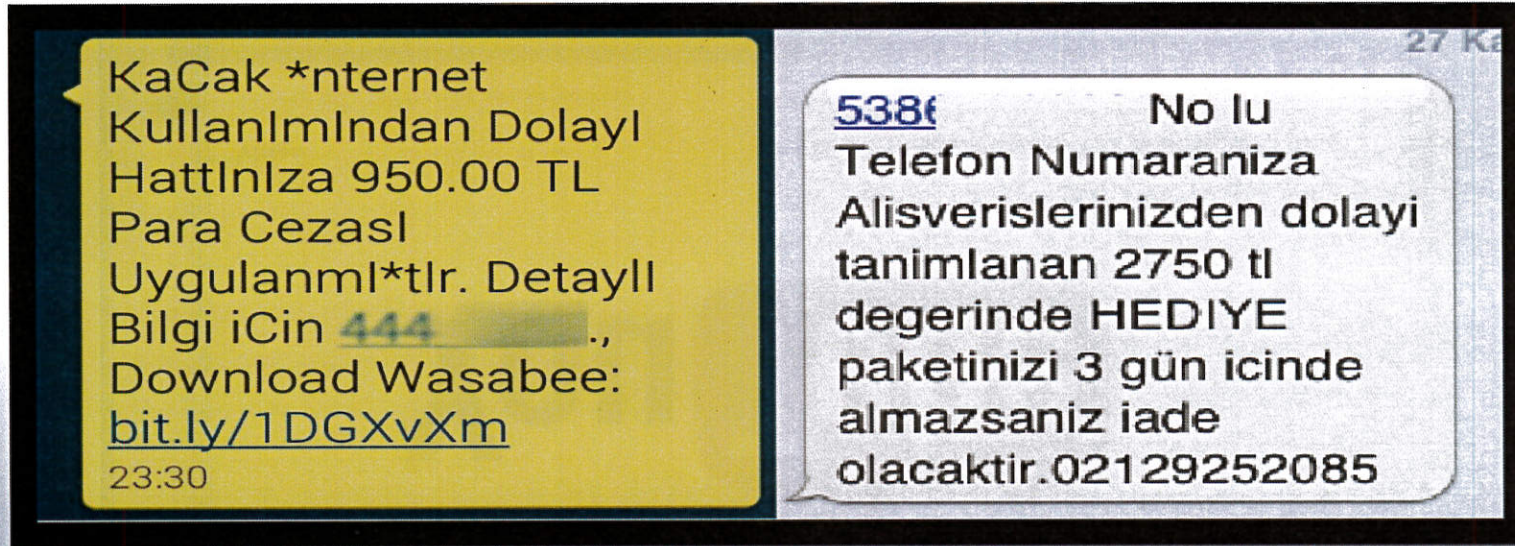
Sosyal Mühendislik

Oltalama



Sosyal Mühendislik

Oltalama



Sosyal Mühendislik

Tarih: 10 Kasım 2010, Çarşamba, 11:41

Gönderen: ahmetzen@golfggrup.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 düzenleneceğini 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.
- **Acilliğin** üzerine vurgu yapılması.
- İsteğin yerine getirilmemesi durumunda kötü sonuçlar doğacağına söylenmesi.
- Soru sorulduğunda rahatsız olunması.
- Bilinen adların sıralanması.
- İltifat edilmesi ve kur yapılması.

Sosyal Mühendislik

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



Eposta Güvenliği

- **Kaynağı bilinmeyen** e-postalar kesinlikle açılmamalıdır.
- İçeriğinden **şüphelenilen** e-postaların kaynağı doğrulanmalı (Örneğin; arkadaşınızdan gelen şüpheli bir e-posta, arkadaşınızı arayıp onaylatmadan açılmamalı!),
- E-posta **ekleri** 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

Yönetici hesabı bildirim kapatma güncelleştirmesi 1 mesaj

Kimden: Teknik destek, sistem yardım masası, 8 Kasım 2017 13:20

 **Kimliğinizi onaylayın.** Hesap bilgiler etmek için hesap bilgilerinizi doğrul sınırını aştı 0,99 GB üzerinde çalışan mümkün olmayabilir, lütfen aşağıda

 **Teknik destek, sistem yardım masası,**
padula@cefetmg.br

posta kutunuzu kullanmaya devam tarafından belirlenen 100 GB depolama kadar zaman yeni e-posta almak

Bilgilerinizi güncellemek için buraya tıklayın: <http://ciechec.ucoz.net/ogrenciposta.karatekin.edu.tr.html>

Son uyarı! 24 saat içinde doğrulanmadı tüm hesapları veritabanımızda bu mesajı yoksayılır silinecektir, biz bu onay için herhangi bir rahatsızlık için özür dileriz.

Teknik destek, sistem yardım masası,
Copyright © | 2017. Çankırı Karatekin Üniversitesi
Tüm hakları saklıdır, Web e-posta yönetim ekibi.

--
Esta mensagem foi verificada pelo sistema de antivírus e acredita-se estar livre de perigo.

Yanıtla - Tümüne Yanıt Ver - İlet - Daha Fazla İşlem

Eposta Güvenliği

Bilgi sınıflandırması ve etiketlemesi; bilgi ve bilgi varlıklarının uygun şekilde muhafaza edilmesi ve işlenmesi için önemlidir. Bilgi sınıflandırması ve etiketlemesi yapılırken aşağıdaki durumlara dikkat edilmelidir;

- Bilgi varlıklarının sahipleri, yaptıkları sınıflandırmadan sorumlu olmalıdır,
- Sınıflandırmadaki koruma düzeyi gizlilik, bütünlük ve erişilebilirlik ve ele alınan tüm gereksinimler analiz edilerek değerlendirilmelidir,
- Sınıflandırma, herkesin bilgi ve ilgili varlıkları aynı şekilde sınıflandırmaları için anlaşılır olmalıdır,
- Her sınıflandırma seviyesi, sınıflandırma uygulaması bağlamında mantıklı bir isme sahip olmalıdır.

Bilgi Sınıflandırma ve Etiketleme

Çok Gizli : Ülke Yönetimi ve üst yönetim tarafından üretilen veya bu makamlar için üretilerek arz edilen, kaybı ya da yetkisiz kişilerin eline geçmesi durumunda çok ciddi sorunların yaşanacağı bilgiler, çok gizli kategorisindedir

Gizli : Kurumun faaliyetini devam ettirebilmesi için kritik olan ve yetkisiz kişilerin eline geçmesi durumunda, risklerin oluşabileceği ve\veya sorunların yaşanabileceği bilgi varlıklarıdır. Gönderilen makamı ilgilendiren, sadece o makamın görebileceği bilgi türüdür.

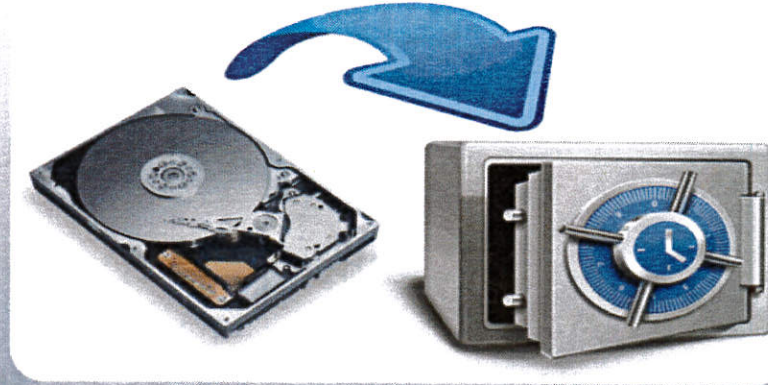
Hizmete Özel : Sadece belli bir grup tarafından, örneğin proje/iş ekipleri, belli bir birim gibi, görülebilecek olan bilgi varlıklarıdır. İçerdiği konular itibariyle, diğer gizlilik dereceli konular dışında olan, ancak güvenlik işlemine ihtiyaç gösteren bilgi varlıkları hizmete özel olarak sınıflandırılır.

Halka Açık : Kullanılması güvenlik açısından önemli olmayan, Kurumdaki veya Kurum dışındaki her kişiye açık bilgilerdir.

Bilgi Sınıflandırma ve Etiketleme

- Yedekleme işlemi; **kaybolma** veya **silinme** tehlikesi olan verilerin başka ortamda kopyalarını bulundurma işlemidir.
- USB Disk, CD, DVD ve benzeri araçlar kullanarak verilerinizin güvenliğini sağlayabilirsiniz.

Yedekleme



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/>



ihbar

