TÜBİTAK
BİLGEM

SOSYAL MÜHENDİSLİK SALDIRILARI

Ünal TATAR

- Herkes bilgi işlem servislerine büyük oranda bağlı.

- Güvenliğin sadece küçük bir yüzdesi teknik güvenlik önlemleri ile sağlanıyor. Büyük yüzdesi ise kullanıcıya bağlı.

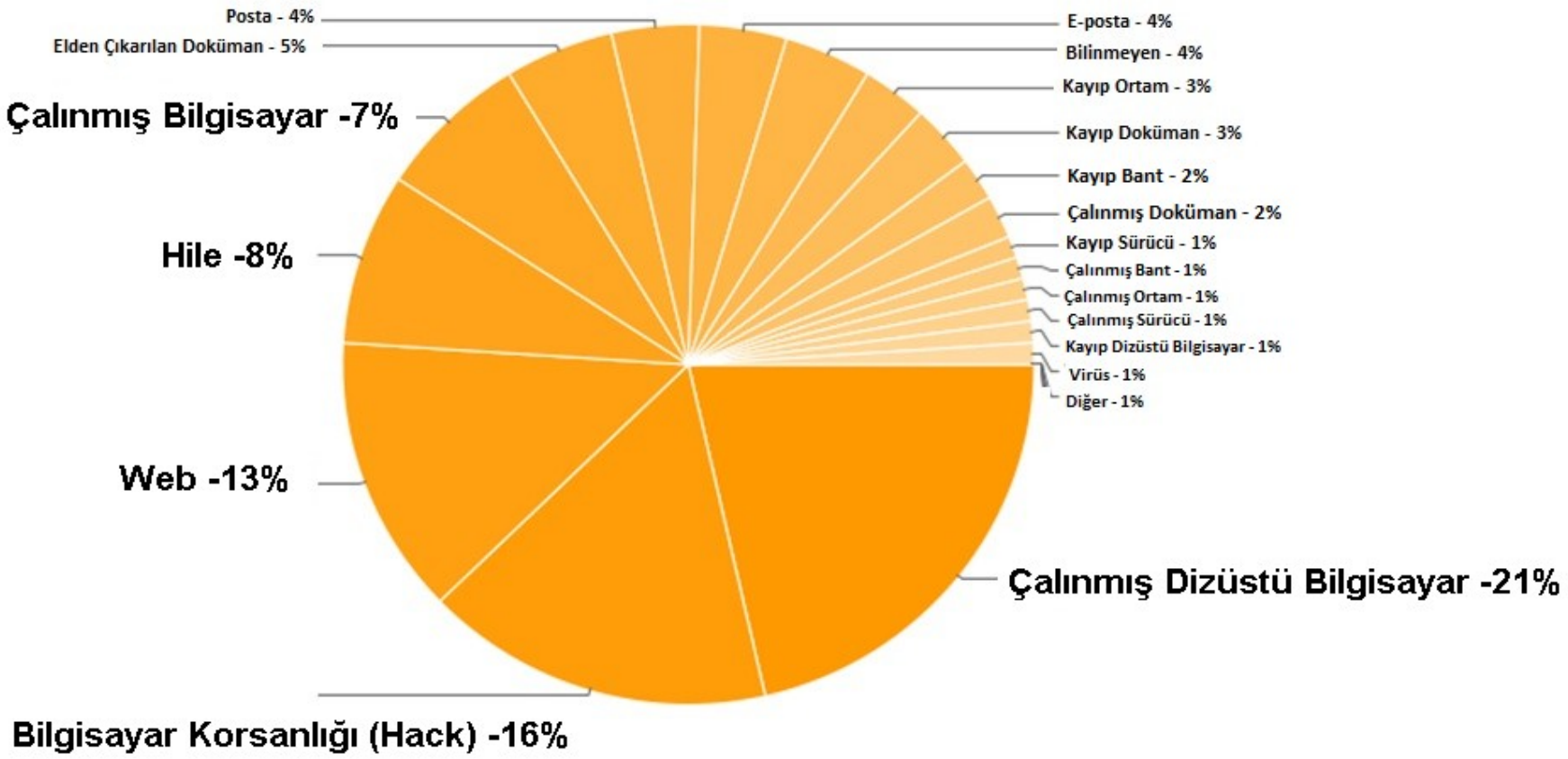
- Pareto prensibi: Alınabilecek önlemlerin %20'sini alarak saldırıların %80'inden korunabilirsiniz.

- Sorumlu herkes:
  - Bilginin sahibi
  - Kullanıcılar
  - Bilgi sistemini yönetenler

- En zayıf halka bilgi güvenliğinin seviyesini belirlemektedir.
- Zincir en zayıf halkası kadar güçlü.
- Çoğunlukla en zayıf halka insandır.

- Bilginiz başkalarının eline geçebilir
- Kurumun onuru, toplumdaki imajı zarar görebilir
- Donanım, yazılım, veri ve kurum çalışanları zarar görebilir

- Önemli veriye zamanında erişememek
- Parasal kayıplar
- Vakit kayıpları
- Can kaybı!



- ABD'de meydana gelen bilgisayar olaylarının türlerine göre dağılımı (2001-2010)

- *Sosyal mühendisler:* Teknolojiyi kullanarak ya da kullanmadan bilgi edinmek için insanlardan faydalanırlar.

- Etkileme ve ikna yöntemlerini kullanırlar.

- Sosyal Mühendislik: Normalde insanların tanımadıkları biri için yapmayacakları şeyleri yapmalarını sağlama sanatı.

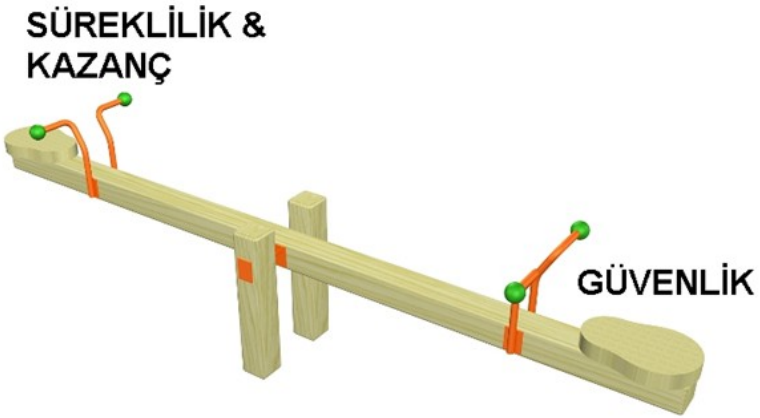
- Teknoloji kullanımından çok insanların hile ile kandırılarak bilgi elde edilmesi

- Kullandığı en büyük silahı, insan zaafiyetleri
- İnsan: Güvenliğin en zayıf halkası
- Symantec: Zararlı yazılımların %90'ı insan etkileşimini gerektirmektedir.
  - Bir e-posta eklentisinin indirilmesi
  - Bir bağlantıya tıklama
  - USB bellek takma

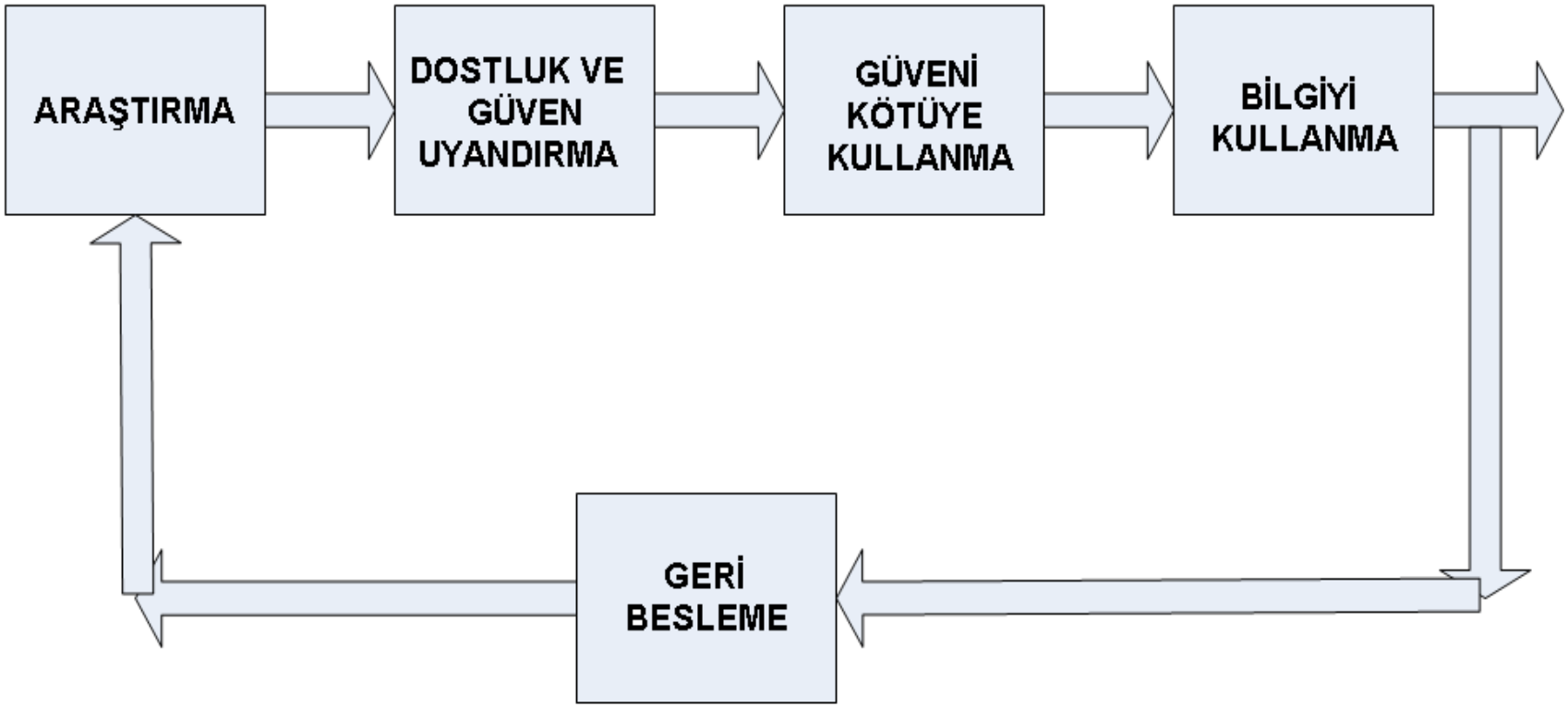
> *"Yalnızca iki şey sonsuzdur, evren ve insanoğlunun aptallığı; aslında evrenin sonsuzluğundan o kadar da emin değilim."*
>
> (Albert Einstein)

- Çoğu insan, kandırılma olasılığının çok düşük olduğunu düşünür.
- Bu ortak inancın bilincinde olan saldırgan, isteğini o kadar akıllıca sunar ki hiç kuşku uyandırmaz ve kurbanın güvenini sömürür.

- Kurum güvenliği denge konusudur.



- En emniyetli bilgisayar?
  - Kapalı olandır(!)
  - Peki şuna ne dersiniz?: Art niyetli bir kişi ofise gidip bilgisayarı açması için birini ikna edebilir.


ARAŞTIRMA
DOSTLUK VE GÜVEN UYANDIRMA
GÜVENİ KÖTÜYE KULLANMA
BİLGİYİ KULLANMA
GERİ BESLEME

- Sahte senaryolar uydurmak
- Güvenilir bir kaynak olduğuna ikna etmek (phishing)
- Truva atları
- Güvenilir bilgi karşılığında para, hediye, vs önermek
- Güven kazanarak bilgi edinmek
- Omuz sörfü, çöp karıştırmak, eski donanımları kurcalamak

- Sosyal mühendislik saldırılarında kullanılabilen bazı donanımlar:

USB bellekli saat
(19.99$)

Donanımsal keylogger
(59.99$)

USB bellekli çakmak
(39.99$)

Kameralı araba anahtarı
(59.99$)

SD kartı saklayıcısı
(20.99$)

Kameralı kalem
(79.99$)

Kameralı gözlük
(79.99$)

Test-Drive SpoofCard (It's Free!)

	country	phone number
Your Number	+1	
Your Friend's Number	+1	
Caller ID to Display	+1	

Embed On Your Site

PLACE FREE CALL

- Saldırgan: *Albert Lim* takma isimli şahıs

- Kurban (kılığına geçmiş şahıs): Ofisten bir arkadaşımız

- Konu: Para

TÜBİTAK BİLGEM

Date: Tue, 15 Sep 2009 11:24:57 -0700
From: limalbert09@golfchannelclub.com
To: you@next.com
Subject: Next Of Kin

Dear Friend

I am Albert Kohl, a Singaporean and a seasoned Accountant with Berhad Office. It is with good spirit of heart I opened up this great opportunity to you; a deceased client of mine that shares the same last name as yours died as a result of heart-related condition on March 12th 2005. His heart condition was due to the death of all the members of his family in the tsunami disaster on the 26th December 2004 in Sumatra Indonesia where they all lost their lives. Currently his account of US$7.300 million with us has been unclaimed due to unavailability of a next of kin/relatives to claim his estate.

Since none of the family relative is alive to claim this fund after, haven waited until now for any relative next of kin to surface in our custody; I decided to contact you fast; so that I can present you as the relative next of kin to my late client before the funds are confiscated. You dont need to worry yourself in this transaction. I will provide the legal documents in your name and favor.

Hence I am seeking your cooperation and understanding to stand as the deceased next of kin to enable us claim the inheritance before the period given elapse.
If you are interested and in agreement with me, get back to me quickly and I will send to you all our contacts and the information you may need to proceed.The proceedings will be shared 35% for you 55% for me and 10% for any expenses we incurred during this process.

Best Regards,
Robert Wilson
albertlim@sify.com

ORIGINAL

FORM D2

ROYAL MALAYSIA
NATIONAL POPULATION COMMISSION

DEATH CERTIFICATE

Issued under the birth and death (compulsory registration) Decree 69 of 1996

Registration centre: KUALA LUMPUR

D NO. 782644
Certificate number

Volume	Year	Entry No
0485	2005	00985

Town: AMPANG

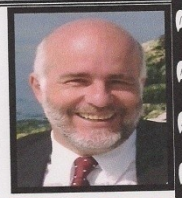
Country: MALAYSIA

This is to certify that death details of which are recorded herein have been registered on

27th	March	2005
Day	Month	Year

at the registration centre.

Full Name: ANDREW KARABACAK



Sex: MALE

Date of Birth:	Day	Month	Year
	9th	August	1944

Age at Death: ~61 YEARS.

Place of Death: ~ MALAYSIA.

Date of Death:	Day	Month	Year
	12th	March	2005

CERTIFIED DEAD

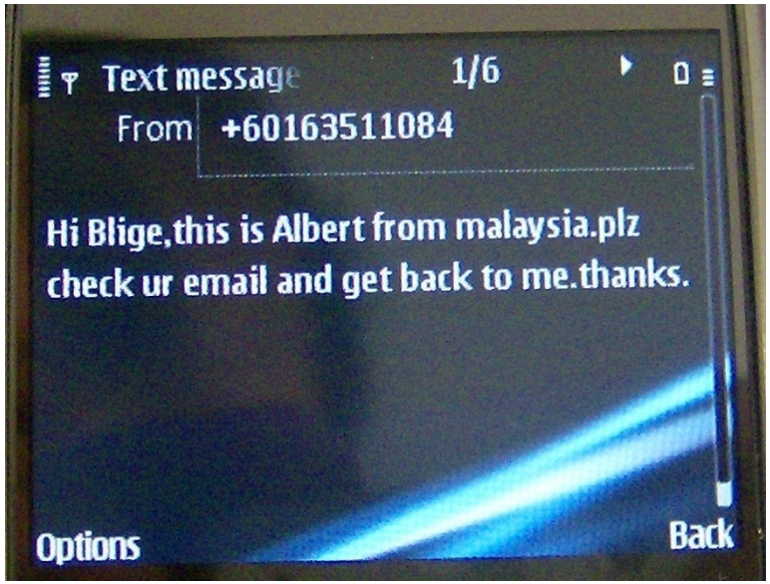
Address of the Deceased: ~ 11 JALAN AMPANG KUALA LUMPUR, MALAYSIA

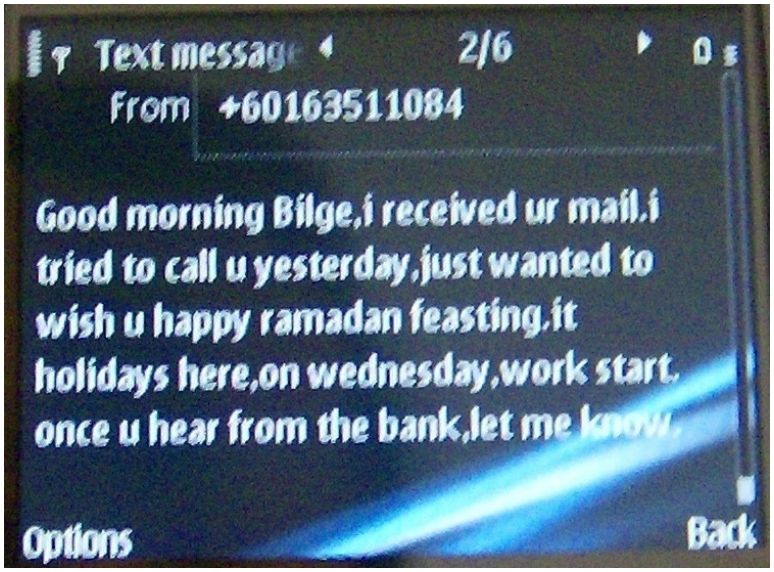
Place of Issue: ~ KUALA LUMPUR MALAYSIA.

Date of Issue:	Day	Month	Year
	27th	March	2005

REGISTRAR:
MRS GRACE KOH HAI

- Farklı tarihlerde saldırgandan gelen SMS'ler





Attention: **THE EXECUTIVE DIRECTOR,**
HSBC BANK, BERHAD
MALAYSIA

E-mail; **hsbcbank@h-s-b-c-online.net**

Sir,

I,……On behalf of my late relative (MR.ANDREW KARABACAK). I am submitting this letter on behalf of the family regards his deposit at your custody; please advise me all necessary processes needed to conclude the release of my inheritance bestowed to me by my late relative valued at US$M7.3(Seven Million three Hundred Thousands United States Dollars.

Yours faithfully,
Name……..
Address…….
Tel:……


HSBC BANK MALAYSIA
MR. ALBERT K. LIM
BERHARD BANGUNAN
HSBC No: 2 LEBOH
AMPANG 50100
CHIEF ACCOUNTANT
OFFICER
HSBC
The world's local bank

Leamington man loses $150,000 in Nigerian scam

BY TREVOR WILHELM, THE WINDSOR STAR JANUARY 14, 2009 COMMENTS (570)

STORY | PHOTOS (1)

An emotional John Rempel tells his story of how he has lost $150,000 of the family's money to a Nigerian scam.

Photograph by: Nick Brancaccio, The Windsor Star

A Leamington man has fallen prey to international scam artists who strung him along for more than a year with the promise of millions in cash, but ultimately bilked him and his family of $150,000.

STORY TOOLS

E-mail this Article

Print this Article

Comments (570)

Share this Article

Font: A A A A

RELATED STORIES

Leamington family fleeced of $150,000

World Report

Local hockey notes

RELATED STORIES FROM SISTER PUBLICATIONS

Little movement in first rankings of the year

Sigara sağlığa zararlıdır …

Bir bankaya yapılan sosyal mühendislik …

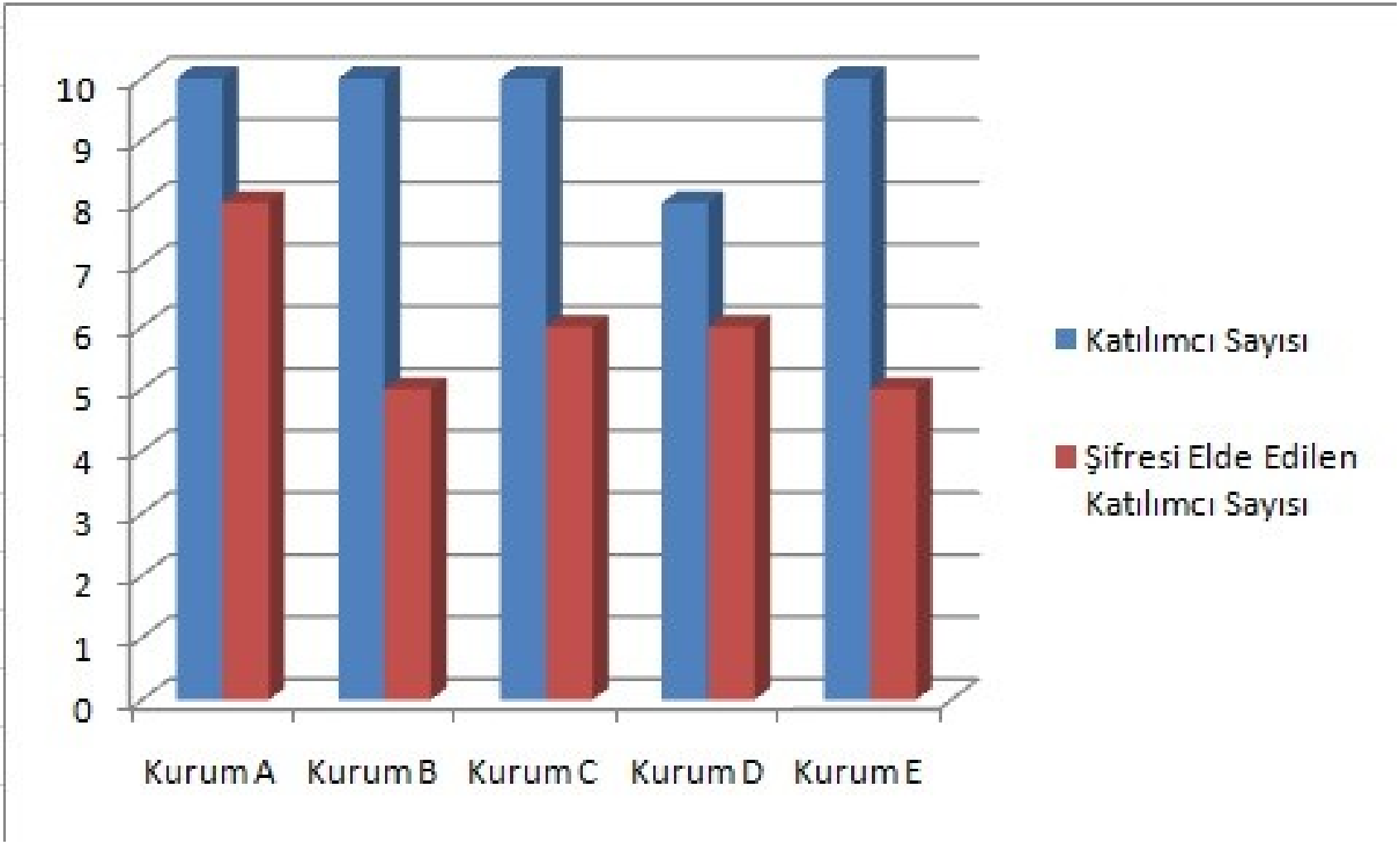
Tarafımızca başka kurumlara yapılan sosyal mühendislik saldırılarından bazı örnekler …

1. ***kayıt:***

2. kayıt:

3. kayıt:

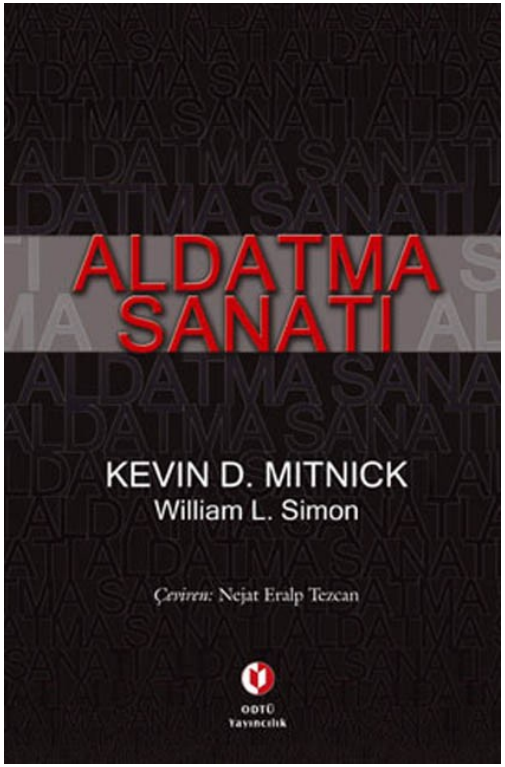
- Kamu kurumlarında durum:



- Yapılan testler sonucunda kullanıcıların yaklaşık %65'inin şifresini ele geçirebildik!

Elde Edilen Bilgisayara Giriş Kullanıcı Adı	Elde Edilen Bilgisayara Giriş Şifresi
0872	444444
1444	683154
1325	mine8
1276	nilem999
1386	ozgeburak7
1094	ŞİFRE VERMİYOR
VERMİYOR	ŞİFRE VERMİYOR
689	ŞİFRE VERMİYOR
1009	1009
1248	ŞİFRE VERMİYOR

- Sosyal Mühendislik Kavramı
- Saldırı Teknikleri
- Sosyal Mühendislik Saldırı Örneği
- Sosyal Mühendislik Testleri
- Korunma Yöntemleri
- Uygulama



- **İçermesi gereken bazı önemli maddeler:**
  - Kurum her an saldırıya maruz kalabilir
  - Sorun sadece teknoloji sorunu değildir
  - Kurumun tüm çalışanları bilgi güvenliğinin bir parçası
  - Eğitimler periyodik olarak düzenlenmeli
  - Prosedürlerin ve uygulamasının önemi
    - Örneğin, şifre oluşturma prosedürü

- Kullanıcı bilinçlendirme eğitimlerinde verilen bilgi, kullanıcılar tarafından yeterli derecede öğrenilmiş mi?
- Ödül ve teşvik amacıyla eğitim sonunda kullanıcılara katılım sertifikası verilebilir.
- Tüm kurum personelinden kurallara uyacağına dair imzalı bir taahhüt belgesi alınabilir.

- Kurumun iç sayfasına bilgi güvenliğiyle ilgili karikatürler, ipuçları koyma
- Ayın güvenlik çalışanının resmi
- Çeşitli bilgi güvenliği posterleri asma
- Bülten panolarına duyurular

- Hatırlatma amaçlı e-postalar
- Bilgi güvenliğiyle ilgili İnternet sitelerinin takibi

- Risk analizi yapılması
  - Kurumun bilgi varlıkları neler?
  - Bu varlıklara ne gibi tehditler var?
  - Bu tehditler gerçekleşirse kuruma ne gibi zararlar gelebilir?
- Veri sınıflandırma
  - Tasnif dışı
  - Hizmete özel (Özel)
  - Gizli

- Kurumda periyodik olarak bilgi güvenliği testleri yapılmalı
- Antivirüs yazılımları mutlaka tüm bilgisayarlara kurulmalı ve tanım dosyası güncel tutulmalı
- Çöpe atılması gereken dokümanlar, kırpıcılardan geçirilebilir

- Şifre korumalı ekran koruyucular kullanılabilir
- Temiz masa / temiz ekran politikası
- İşten ayrılan çalışanların uyması gerektiği prosedürler hazırlanabilir
- Kuruma ziyaretçi olarak gelen kişilerden kimlik alınabilir, kurum içerisinden bir çalışan bu kişiye refakat edebilir

- Tehlike hiç ummadığınız bir anda, hiç ummadığınız bir yerden gelebilir.
- Tanımadığınız kişilerden gelen isteklere karşı temkinli davranın.
- Size özel bilginizi (örneğin şifreniz) kimseyle paylaşmayın.
  - Sistem yöneticisi
  - Yan masada oturan mesai arkadaşınız
  - Hatta yöneticileriniz

- Kurumdaki tüm personele periyodik olarak bilgi güvenliği bilinçlendirme eğitimleri verin.
- Kurumunuzda periyodik olarak, sosyal mühendislik saldırı testini de içeren, bilgi güvenliği testleri gerçekleştirin.

TÜBİTAK BİLGEM

TÜBİTAK-BİLGEM-UEKAE

Bilişim Sistemleri Güvenliği Bölümü

tatar@uekae.tubitak.gov.tr

0 312 427 73 66

www.bilgiguvenligi.gov.tr

www.bilgimikoruyorum.org.tr