TÜBİTAK

Kullanıcı Güvenliği Eğitimi

TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü

Sunum İçeriği

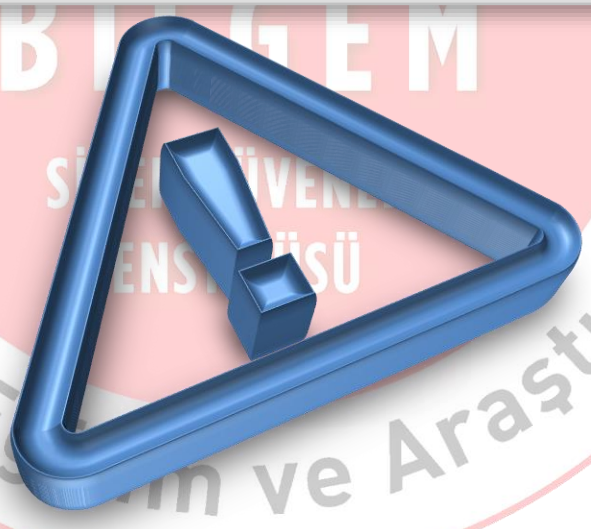
- Amaç
- Sorumluluk
- Bilgisayar ve Erişim Güvenliği
- Parola Güvenliği
- Yazılım Yükleme ve Güncelleme
- Dosya Erişim ve Paylaşım Güvenliği
- Zararlı Yazılımlar
- Sosyal Mühendislik
- Web ve E-posta Güvenliği
- Mobil Cihaz Güvenliği
- Yedekleme

Amaç

Amaç

"Yazılı ve elektronik ortamdaki kurumsal bilgiyi korumak"

- Gizli (yetkisiz kullanıcılar görmesin!)
- Bütün (bilgi bozulmasın! başkası tarafından değiştirilmesin!)
- Erişilebilir (yetkili kullanıcılar ihtiyaç duydukları an görebilsin!)



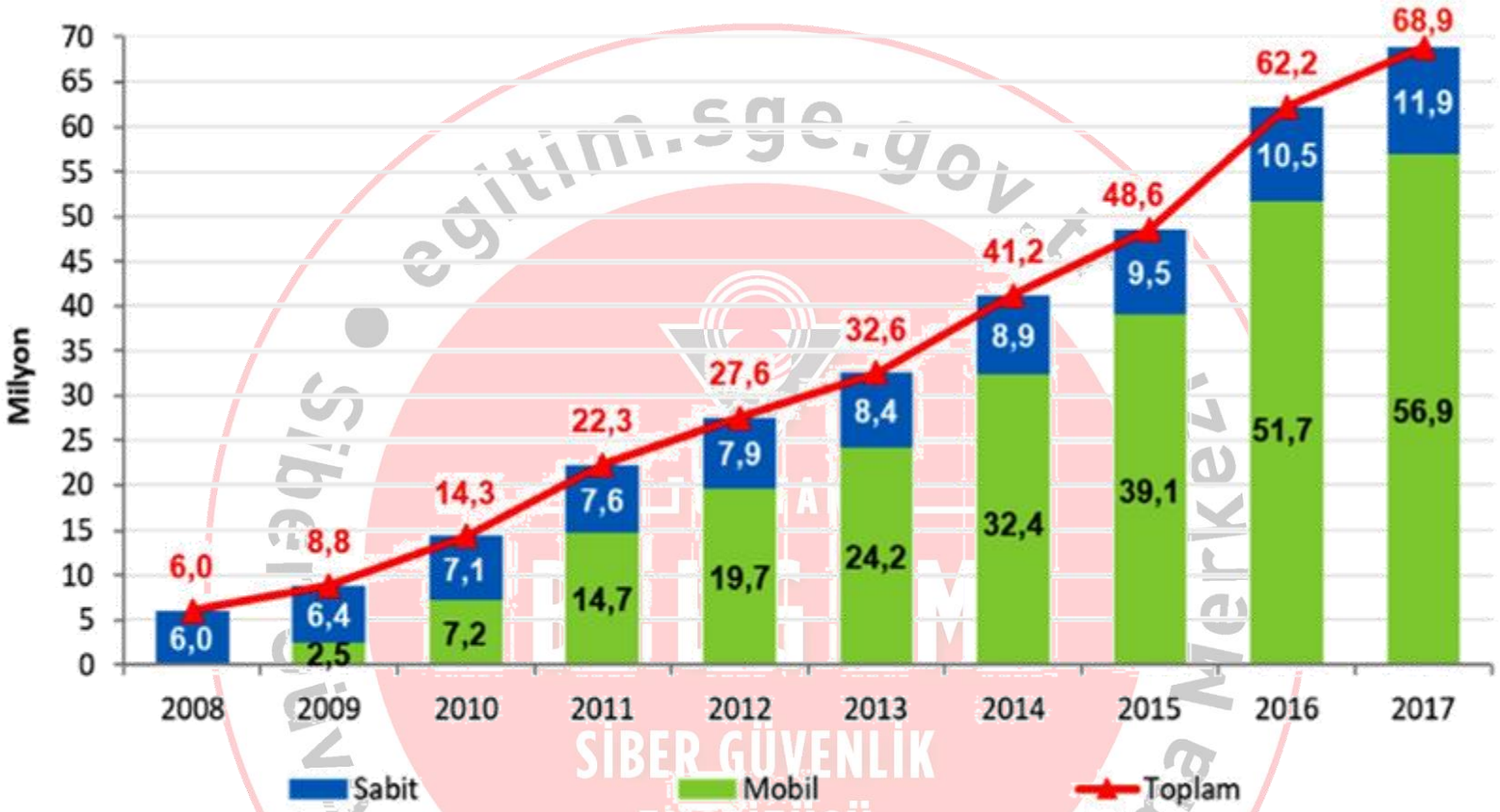
Ya da, kurum olağan işleyişini gerçekleştiremez ve itibar kaybeder.

Bilgi Güvenliği Nedir?

- Bilgi güvenliği, kurumsal bilginin
  - Gizliliğinin,
  - Bütünlüğünün ve
  - Erişilebilirliğinin

  sağlanmasıdır.

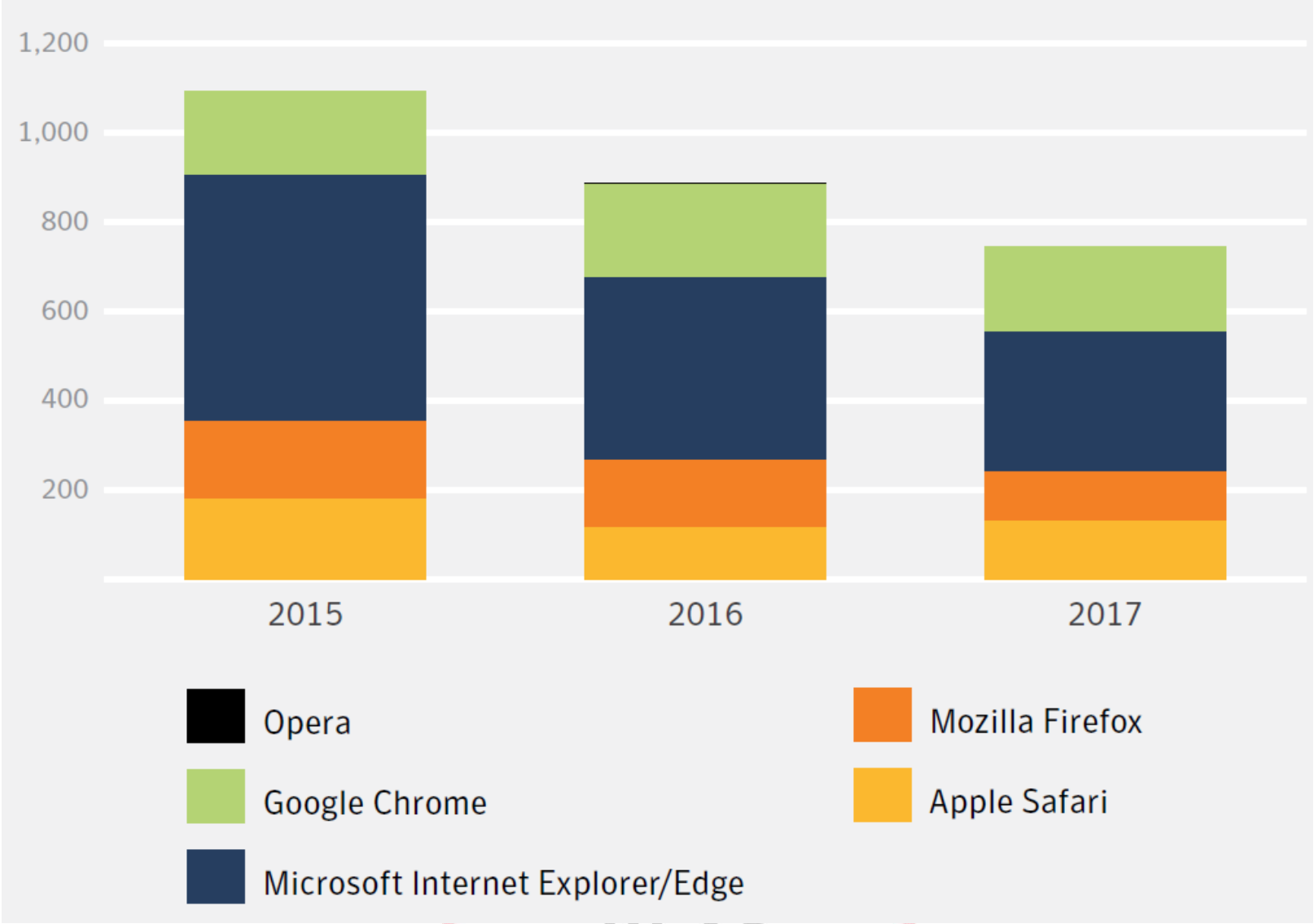
Siber Uzay (Internet)



Türkiye'deki 2017 yılı dördüncü çeyrek sonu Genişbant İnternet Abone Sayısı

BTK Pazar Verileri Raporu, 2017-4.
https://www.btk.gov.tr/uploads/pages/2017-q4.pdf

İnternet Tarayıcılardaki Açıklıklar



Internet Security Threat Report – ISTR Volume 23 - 2018 - Symantec

ABD’de gerçekleşen en kapsamlı DDoS Saldırısı

- 20 Ekim 2016 tarihinde gerçekleştiriliyor.
- Kullanılan zararlı yazılımın adı “Mirai”, “Mirai Botnets”

Kaynak:

http://www.computerworld.com/article/3135434/security/ddos-attack-on-dyn-came-from-100000-infected-devices.html
https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/
https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/
https://www.a10networks.com/blog/dyn-ddos-attack

ABD’de gerçekleşen en kapsamlı DDoS Saldırısı

- Ayrıca ABD hükümetine ait kurum ve kuruluşların sitelerinin de çöktüğü belirtiliyor.
- Ülkenin yüzde 78'inden fazlasının internetsiz kaldığı belirtiliyor.
- Maddi zararın ise 7 milyar doları bulduğu ifade ediliyor.
- Saldırı Rusya ve Çin üzerindeki 14 milyondan fazla IP adresinden Amerika Birleşik Devletleri hedef alınarak yapılıyor.
- Cuma günü yapılan saldırı için yaklaşık 100.000 adet cihaz kullanıldığı tahmin ediliyor.
- Çarşamba günü Mirai zararlı yazılımının yaklaşık 500.000 cihaza bulaştığı ifade ediliyor.

Mirai Botnet Saldırısında kullanılan Parolalar

```
1   // root      xc3511      // root      vizxv          // root      admin
2   // admin     admin       // root      888888         // root      xmhdipc
3   // root      default     // root      juantech       // root      123456
4   // root      54321       // support   support        // root      (none)
5   // admin     password    // root      root           // root      12345
6   // user      user        // admin     (none)         // root      pass
7   // admin     admin1234   // root      1111           // admin     smcadmin
8   // admin     1111        // root      666666         // root      password
9   // root      1234        // root      klv123         // Administrator admin
10  // service   service     // supervisor supervisor    // guest     guest
11  // guest     12345       // guest     12345          // admin1    password
12  // administrator 1234    // 666666    666666         // 888888    888888
13  // ubnt      ubnt        // root      klv1234        // root      Zte521
14  // root      hi3518      // root      jvbzd          // root      anko
15  // root      zlxx.       // root      7ujMko0vizxv   // root      7ujMko0admin
16  // root      system      // root      ikwb           // root      dreambox
17  // root      user        // root      realtek        // root      00000000
18  // admin     1111111     // admin     1234           // admin     12345
19  // admin     54321       // admin     123456         // admin     7ujMko0admin
20  // admin     1234        // admin     pass           // admin     meinsm
21  // tech      tech
```

IoT Saldırılarında Kullanılan Kullanıcı Adı ve Parolalar

IoT Saldırılarında En Çok Kullanılan Kullanıcılar

Rank	2017 User Name	2017 Percent	2016 User Name	2016 Percent
1	root	40	root	33.5
2	admin	17.3	admin	14.1
3	enable	10.3	DUP root	6
4	shell	10.2	DUP admin	2.1
5	guest	1.5	ubnt	1.3
6	support	1.3	test	1.1
7	user	1.1	oracle	1.1
8	ubnt	0.9	postgres	0.7
9	DUP root	0.6		0.7
10	supervisor	0.5	123321	0.6

IoT Saldırılarında En Çok Kullanılan Parolalar

Rank	2017 Password	2017 Percent	2016 Password	2016 Percent
1	system	10.3	admin	9.5
2	sh	10.2	root	5.8
3	123456	9.1	12345	5
4	admin	3.7	123456	3.7
5	1234	3.1	password	3.2
6	password	2.5	1234	2.4
7	12345	2.5	ubnt	1.7
8		2.3	admin123	1
9	root	2.1	abc123	0.9
10	support	1.2	pass	0.7

Ülkelere göre IoT Saldırılar Kaynakları

Rank	Country	2017 Percent	Country	2016 Percent
1	China	21	China	22.2
2	United States	10.6	United States	18.7
3	Brazil	6.9	Vietnam	6
4	Russian Federation	6.4	Russian Federation	5.5
5	India	5.4	Germany	4.2
6	Japan	4.1	Netherlands	3
7	Turkey	4.1	United Kingdom	2.7
8	Argentina	3.7	France	2.6
9	South Korea	3.6	Ukraine	2.6
10	Mexico	3.5	Argentina	2.5

Internet Security Threat Report – ISTR Volume 23 - 2018 - Symantec

Bir Bilgisayar Virüsünün Analizi - Stuxnet

http://vimeo.com/25118844

50 milyon Türk vatandaşının kimlik bilgileri sızdırıldı

Sorumluluk

Düşünce Tuzakları

- Güvenlikten bilgi işlem sorumludur.
- Antivirüs yazılımımız var, dolayısıyla güvendeyiz!
- Kurumumuz güvenlik duvarı (firewall) kullanıyor, dolayısıyla güvendeyiz!
- Bilgimin kopyasını alıyorum, güvenlikten bana ne!
- Bir çok güvenlik saldırısı kurum dışından geliyor!

Bunu biliyor muydunuz?

Internete bağlı ve güvenlik tedbirleri alınmayan bir bilgisayara zararlı yazılımların bulaşma hızı nedir biliyor musunuz?

En fazla 5 dakika.

Bilgi Güvenliğinden Herkes Sorumludur

- Sorumlu herkes!
  - Bilginin sahibi
  - Bilgiyi kullanan
  - Bilgi sistemini yöneten
- Bilgi güvenliğinin seviyesini en zayıf halka belirlemektedir.
- Çoğunlukla en zayıf halka insandır.

When it Comes to Cybersecurity We're all in it Together!

«Our Shared Responsibility»

The United States Department of Homeland Security

Bilgisayar ve Erişim Güvenliği

Kullanıcı Kimliği – Kullanıcı Adı

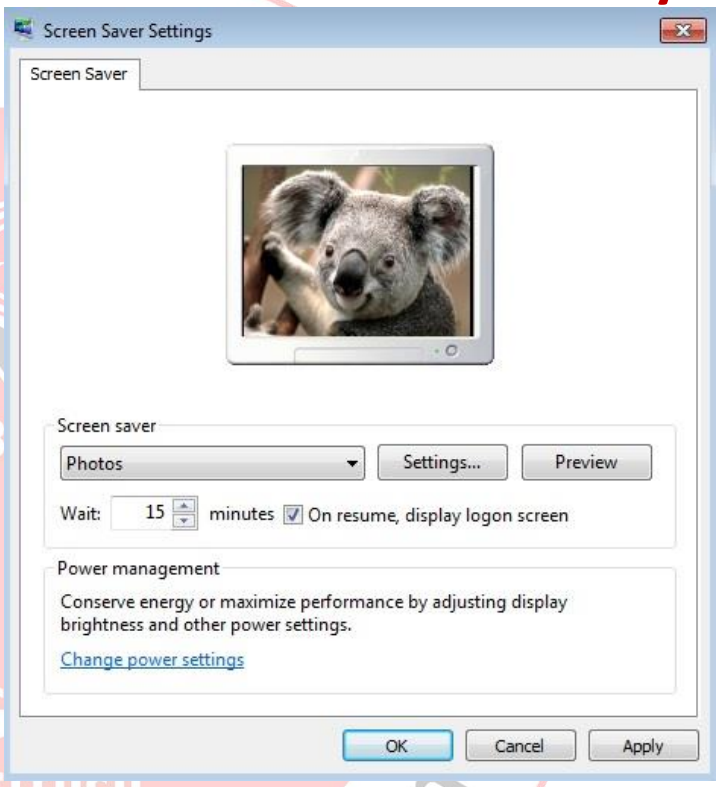
- Parolanın başkaları tarafından ***görülmemesi*** sağlanmalıdır.
- Sizden başka bir kimse kullanıcı hesabınızla işlem yapmamalıdır.

- Parolalarınızı korumazsanız başkalarının günahını da üstlenmek zorunda kalabilirsiniz …

Bilgisayarı Kullanırken

Ekran kilidi

Parola korumalı ekran koruyucusu



Parola Güvenliği

Parola (Şifre) Güvenliği

https://www.youtube.com/watch?v=yo0YTgJzTUY

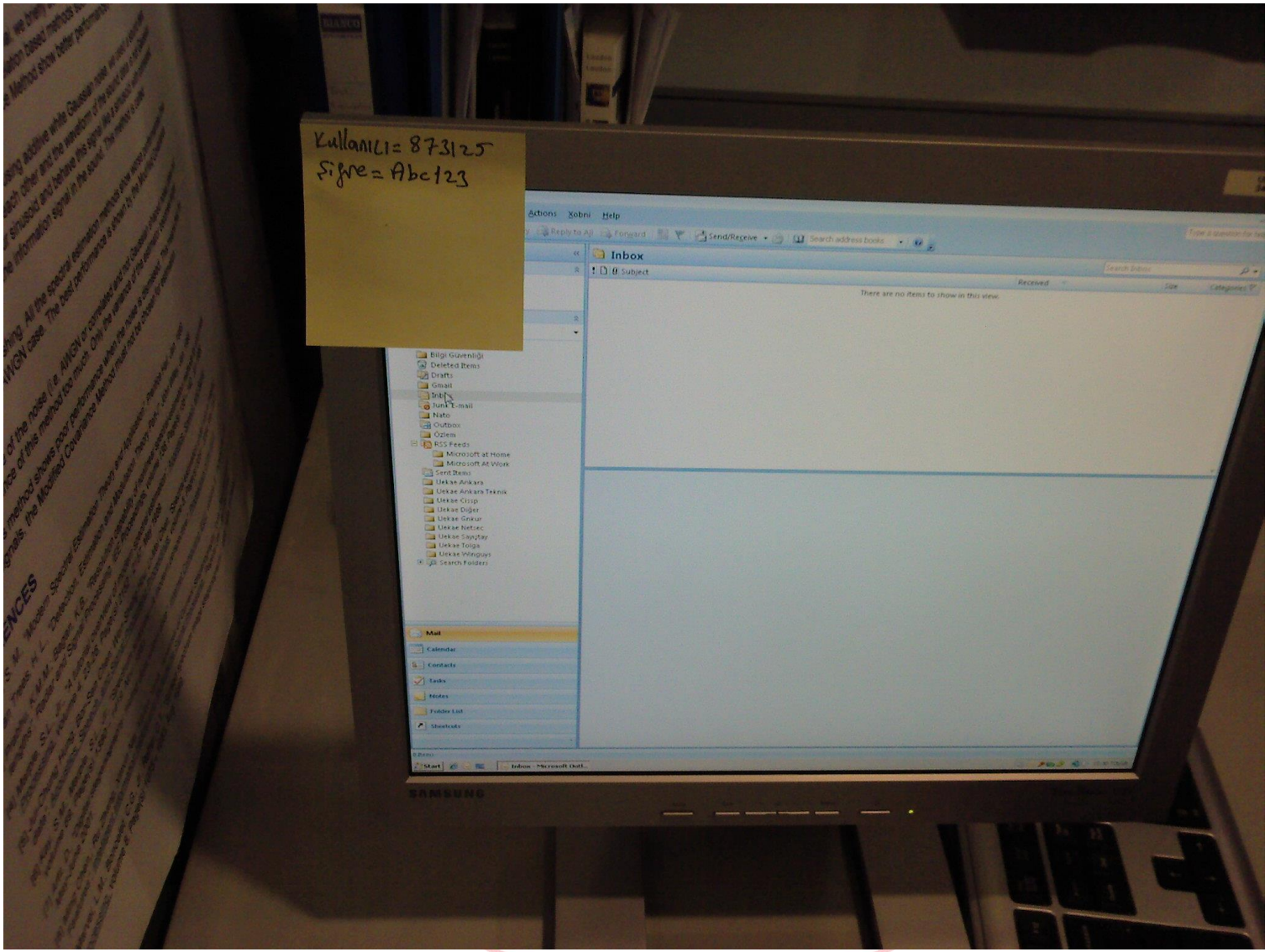
Bankalararası Kart Merkezi

Omuz Sörfü

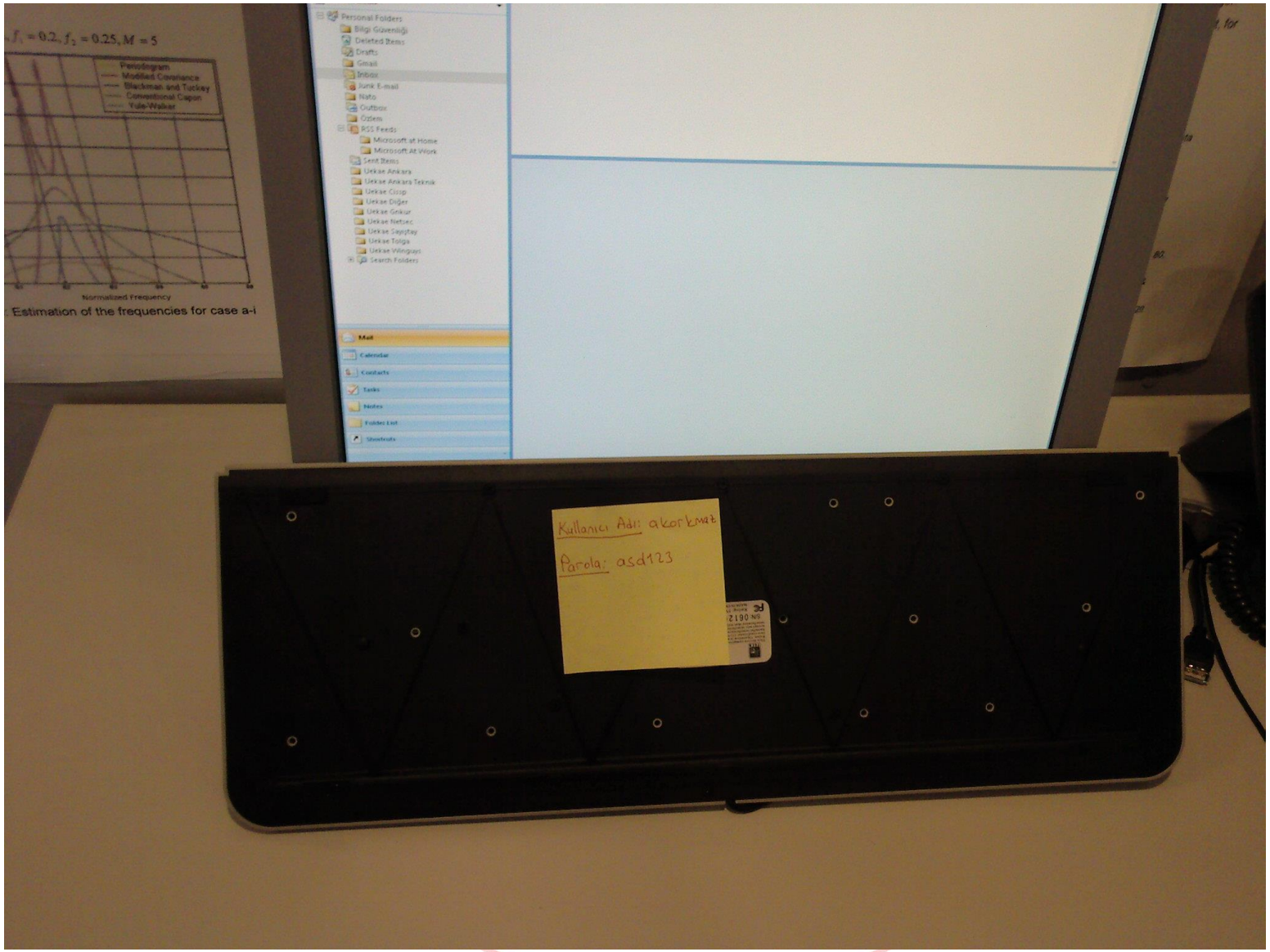
Parola Güvenliği

- En önemli kişisel bilgi, parolanızdır.
- Hiç kimseyle herhangi bir şekilde paylaşılmamalıdır.
- Mümkünse bir yere yazılmamalıdır. Yazılması gerekiyorsa güvenli bir yerde muhafaza edilmelidir.
- Güvenli olmadığını düşündüğünüz mekanlarda kurumsal parolalarınızı kullanmanızı gerektirecek uygulamaları kullanmayınız.

Parolalar - Güvenli Muhafaza Edin



Parolalar - Güvenli Muhafaza Edin



Güçlü parola (şifre) tarifi

İçindekiler

- 2 adet **BÜYÜK HARF** (A, B, C, …)
- 2 adet **küçük harf** (z, y, v, …)
- 2 adet **Sayı** (0, 1, 2, …, 9)
- 2 adet **Özel Karakter** (?, @, !, #, %, +, -, *, %)

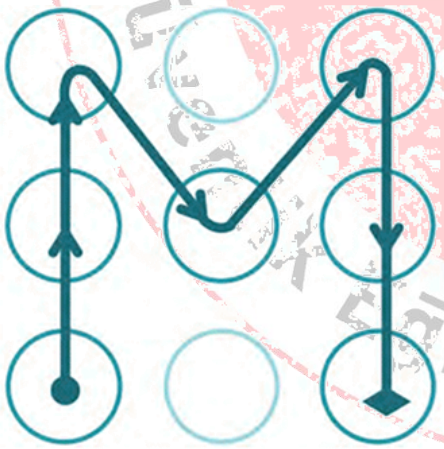
toplamda **en az 8** karakter uzunluğunda.

Bilinen

MT1955@@zym123**

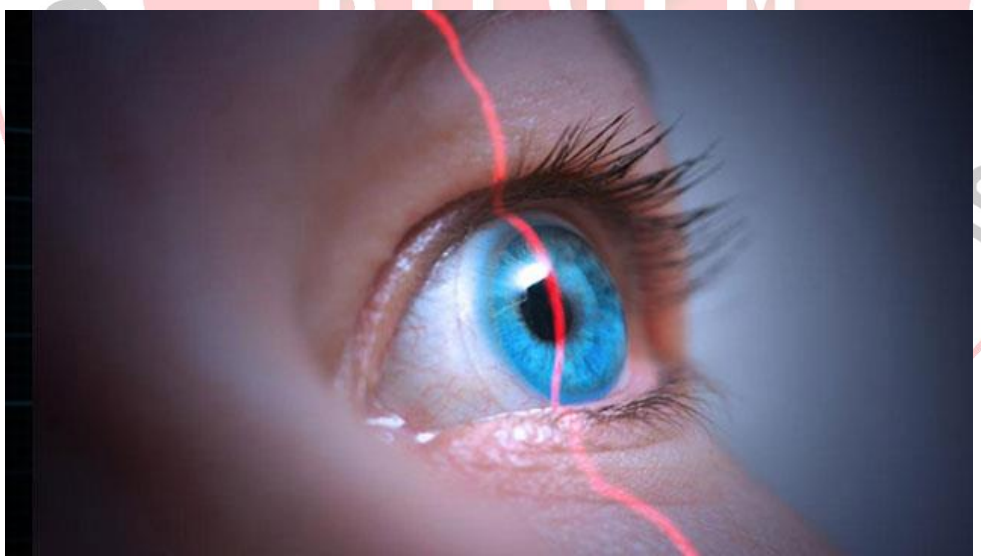
Bir elin nesi var, iki elin sesi var. --> **1Env,2Esv.**

10 Yılda 15 milyon genç yarattık her yaştan. --> **10Y15mgyhy.**



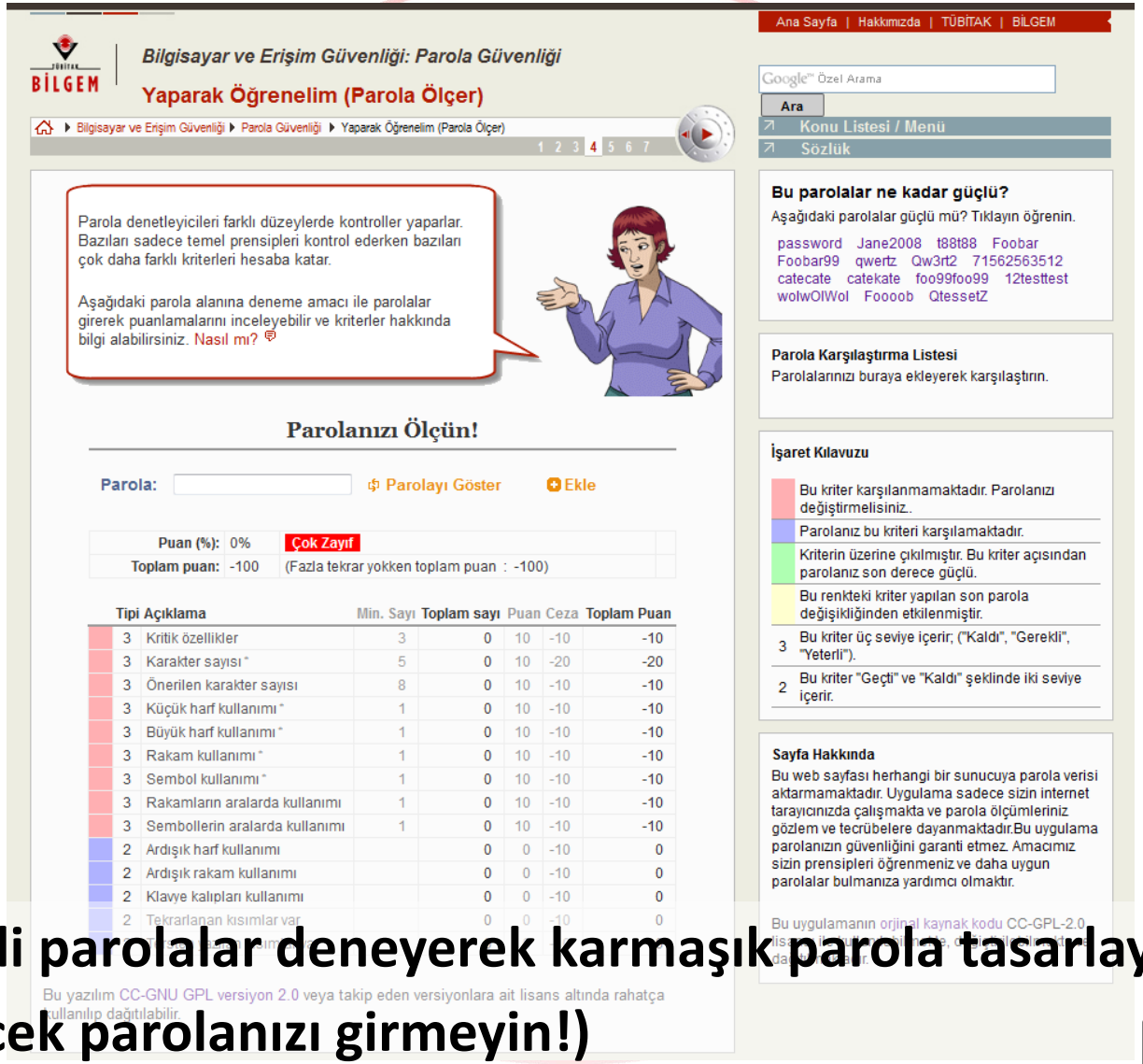
Sahip Olunan

Bizim olan



Parolanızı Deneyin: Parola Ölçer

http://**www.bilgimikoruyorum.org.tr**/?b223_yaparak_ogrenelim



- **Çeşitli parolalar deneyerek karmaşık parola tasarlayın.**
- **(Gerçek parolanızı girmeyin!)**

Parola Güvenliği

- Kişisel bilgilerle ilişkili mi? (çocuğunuzun ismi, evlenme yıldönümü, doğum günü vs.).
- Oyun siteleri, alışveriş siteleri vb. parolalarınızla aynı mı/ benzer mi?
- Tüm sistemlerde aynı parolayı mı kullanıyorsunuz?

Parola Güvenliği – Sizce nasıl?

celik	**Kullanıcının soyismi. 8 karakterden az. Sadece harfler kullanılmış. Özel karakterler, rakamlar kullanılmamış.**
alicelik	**Kullanıcının adı ve soyadı**
Ali_celik1234	**İçerisinde kullanıcı ismi ve soyismi geçiyor.**
ali123	**Kullanıcı isminin türevi de zayıf bir paroladir. 8 karakterden az.**
antalya	**Özel isim. Kullanıcının doğum yeri ise zayıf bir paroladir.**
34bg356	**Araç plakası**
13nisan1967	**Doğum tarihi ya da önemli bir tarih.**
Qwerty123	**Çok kullanılan karakter sıraları.**
Mercedes	**Özel isim**
Kalem	**Sözlüklerde bulunan bir kelime , 8 karakterden az.**
Kalem111	**Kelimenin türevi**

Parola Güvenliği –Bir Kurumun Zayıf Parola Örnekleri

Parola	Adet
1234567	82
qwertyu	55
7654321	3
1234567a	3
12345678	3
1306100	2
zzzzzzz	1
besiktas	1
kurtadam	1

Parola Güvenliği –Zayıf Parolalar vs Kırılma Oranları

Parola	Adet
123456	11
uzak2013	8
111111	3
abc123	3
al1907ex	3
12345678	2
0,0,0,	2

Parola Kırılma Oranı	
Toplam	513
Kırılan	239
Yüzde (%)	46,59

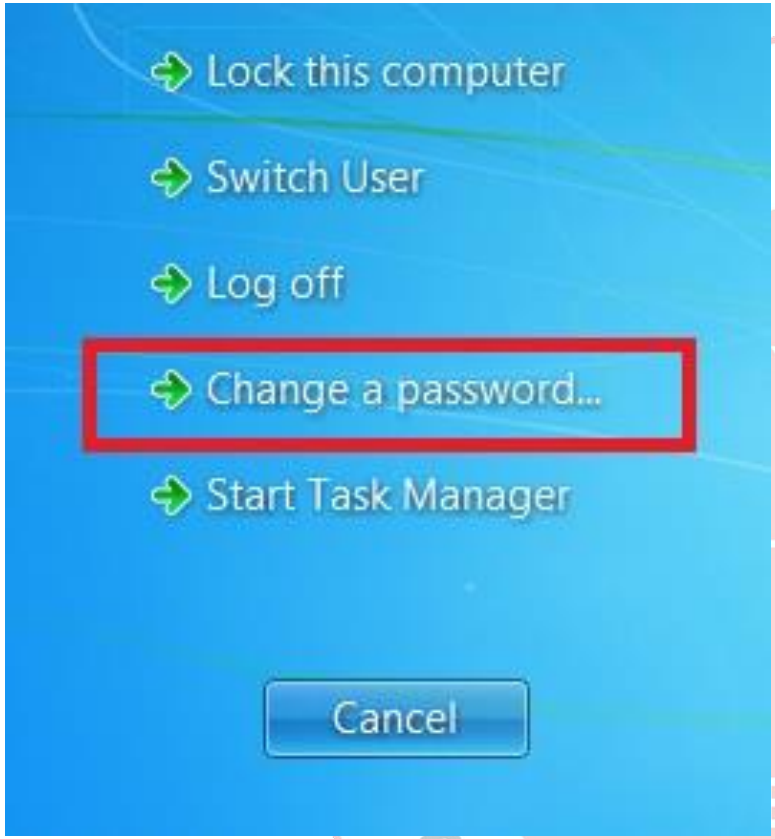
Parola Güvenliği

1234567890	123456789	12345678	1234567	123456	12345
1234	123				
99999999	88888888	77777777	66666666		
9999999	8888888	7777777	6666666		
999999	888888	777777	666666		
99999	88888	77777	66666		
9999	8888	7777	6666		
999	888	777	666		
99	88	77	66		
9	8	7	6		
55555555	44444444	33333333	22222222		
5555555	4444444	3333333	2222222		
555555	444444	333333	222222	xxx	qqqqq
55555	44444	33333	22222	aaa	sql
5555	4444	3333	2222	home	work
555	444	333	222	private	market
55	44	33	22	student	account
5	4	3	2	unknown	anything
11111111	00000000	0987654321		money	campus
1111111	0000000	987654321		nobody	codeword
111111	00000	87654321		secure	public
11111	0000	7654321		superuser	share
1111	000	654321		owner	backup
111	00	54321		manager	temporary
11		4321		Internet	internet
1		321		work123	home123
		21		abc123	pw123
		12		admin123	admin12
				default	foobar
				test	rootroot
				pass	Login
				zxcvbn	zxcvb
				q1w2e3	qweasdzxc
				qweasd	qwerty
				Admin	admin
				123asd	123qwe

qqqq	qqq	aaaaa	aaaa	
file	web	foo	job	
intranet	controller	killer	games	
coffee	cookie	forever	freedom	
academia	files	windows	monitor	
letitbe	letmein	domain	access	
explorer	exchange	customer	cluster	
codename	changeme	desktop	security	
system	shadow	office	supervisor	
super	secret	server	computer	
database	lotus	oracle	business	
ihavenopass	nothing	nopassword	nopass	
example	sample	love123	boss123	
mypc123	temp123	test123	qwe123	
root123	pass123	pass12	pass1	
admin1	password123	password12	password1	
foofoo	temptemp	temp	testtest	
root	adminadmin	mypassword	mypass	
login	Password	password	passwd	
zxccxz	zxcxz	qazwsxedc	qazwsx	
asdfgh	asdzxc	asddsa	asdsa	
qweewq	qwewq	nimda	administrator	
alb2c3	lq2w3e	1234qwer	1234abcd	
123abc	123321	12321	123123	

Conficker *solucanının denediği parola örnekleri!*

Parola Güvenliği – Düzenli olarak değiştirilmeli



Parola Güvenliği – Düzenli olarak değiştirilmeli

Parola Güvenliği - Düzenli olarak değiştirilmeli

Bilin bakalım parola nedir?

Tabii ki

1453

Parola Güvenliği

Parolalar **sakız** gibidir …

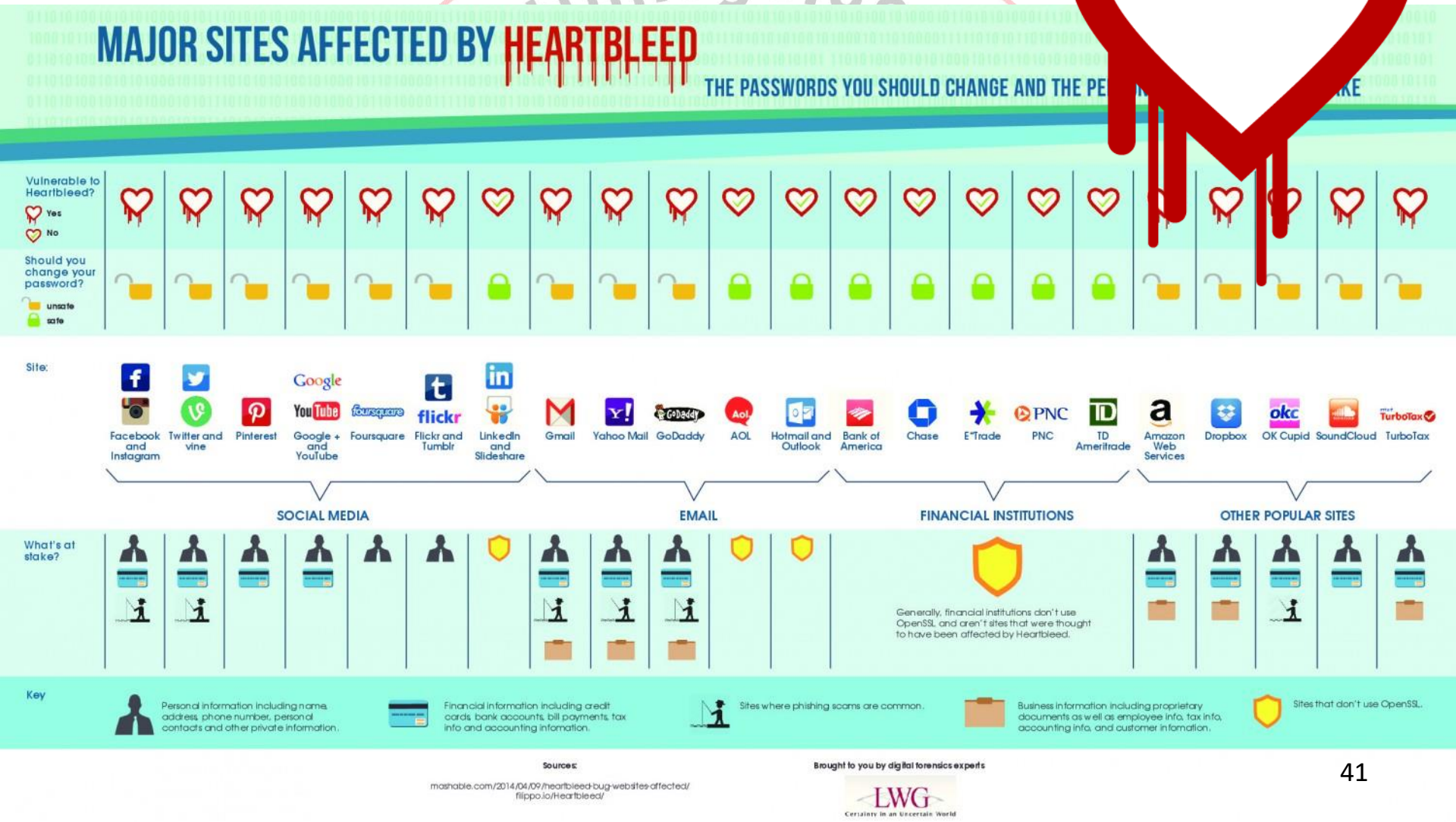
Başkalarıyla **paylaşılmaz**,

ara sıra **yenilemek** gerekir,

ortalıkta bırakılmaz.

OpenSSL Heartbleed Açıklığı

Parolalarınızı değiştirmelisiniz!



Twitter Duyurusu

Hesabını Güvende Tutmak

Twitter hesabın için şifre belirlediğinde, şirketteki kimsenin görmemesi için bir maskeleme teknolojisi kullanırız. Geçtiğimiz günlerde, şifreleri maskelenmemiş olarak dahili günlükte saklayan bir hata belirledik. Hatayı düzelttik ve araştırmalarımıza göre herhangi biri tarafından bir ihlal veya kötüye kullanım söz konusu değil.

En kötü ihtimali düşünerek, bu şifreyi kullandığın tüm hizmetlerde şifreni değiştirmeni rica ediyoruz. Daha fazla bilgi al

Yazılım Yükleme ve Güncelleme

Yazılım Yükleme - Güncelleme

- Her bir programın açıklık oluşturma ihtimali vardır.
- Güvenilir olmayan sitelerden indirilen yazılımlar indirilmemeli ve kullanılmamalıdır.

Yazılım Yükleme - Güncelleme

Güvenli olmayan yazılımlar nelerdir?

- korsan yazılımlar,
- korsan müzik ve film dosyaları,
- kırılmış (crack) programlar ve yazılımlar ile
- kaynağını bilmediğiniz yerden edindiğiniz herhangi bir program.

Riskler

Açıklıklar

"Open Source Security Bug Bounty"

Dosya Erişim ve Paylaşım Güvenliği

Dosya Erişim ve Paylaşım Güvenliği

- Oluşturulan dosyaya erişecek kişiler ve hakları "bilmesi gereken" prensibine göre belirlenmelidir.
- Erişecek kişilerin hakları yazma, okuma, değiştirme ve çalıştırma yetkileri göz önüne alınarak oluşturulmalıdır.
- Verilen haklar belirli zamanlarda kontrol edilmeli, değişiklik gerekiyorsa yapılmalıdır.
- Eğer paylaşımlar açılıyorsa ilgili dizine sadece gerekli haklar verilmelidir.

Dosya Erişim ve Paylaşım Güvenliği

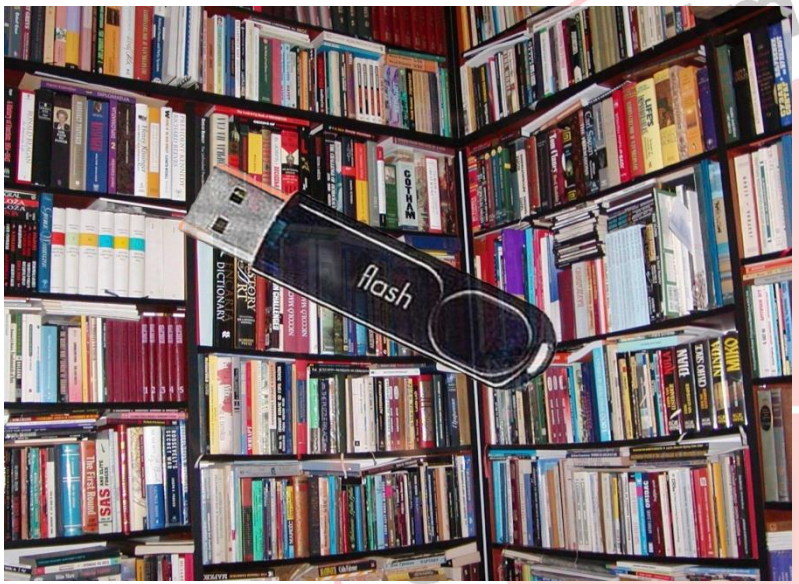
Paylaştırılmış klasörlerden gelebilecek tehlikeler nelerdir?

- Sizin haberiniz olmadan aynı ağdaki bir kişi paylaştığınız dosyalara **erişebilir, değiştirebilir hatta silebilir,**
- paylaşımlar çoğu zaman **virüslerin ve zararlı yazılımların** yayılmak için kullandıkları alanlardır,
- bir dosyanın telif haklarını ***isteyerek veya istemeyerek*** ihlal etmiş olabilir ve yasaları çiğnemiş olabilirsiniz.

Dizüstü Bilgisayar Kullanımı

- Çalınmalara karşı fiziksel güvenlik sağlanmalıdır.
- BIOS ayarlarını başkasının değiştirmesini engellemek için BIOS girişe şifre tanımlanmalıdır.
- Parola güvenliği sağlanmış olmalıdır.
- Bilgiler, bilginin kritikliğine göre gerekirse şifreli saklanmalıdır.
- Bitlocker ile tüm disk şifrelenebilir. (Windows 7 Enterprise sürümü ile birlikte gelir.)

Saklama Ortamlarının Doğru Kullanımı



- USB diskler, bellekler, CD vb.
- Başkaları ile paylaşıldığında bu ortamlar içerisinde gereğinden fazla bilgi bulunmamalıdır.
- İşlevi sona ermiş taşınabilir medya içindeki bilgi tekrar ortaya çıkarılamayacak şekilde yok edilmelidir.
- Taşınabilir medya, masa gibi açık alanlarda bırakılmamalıdır.

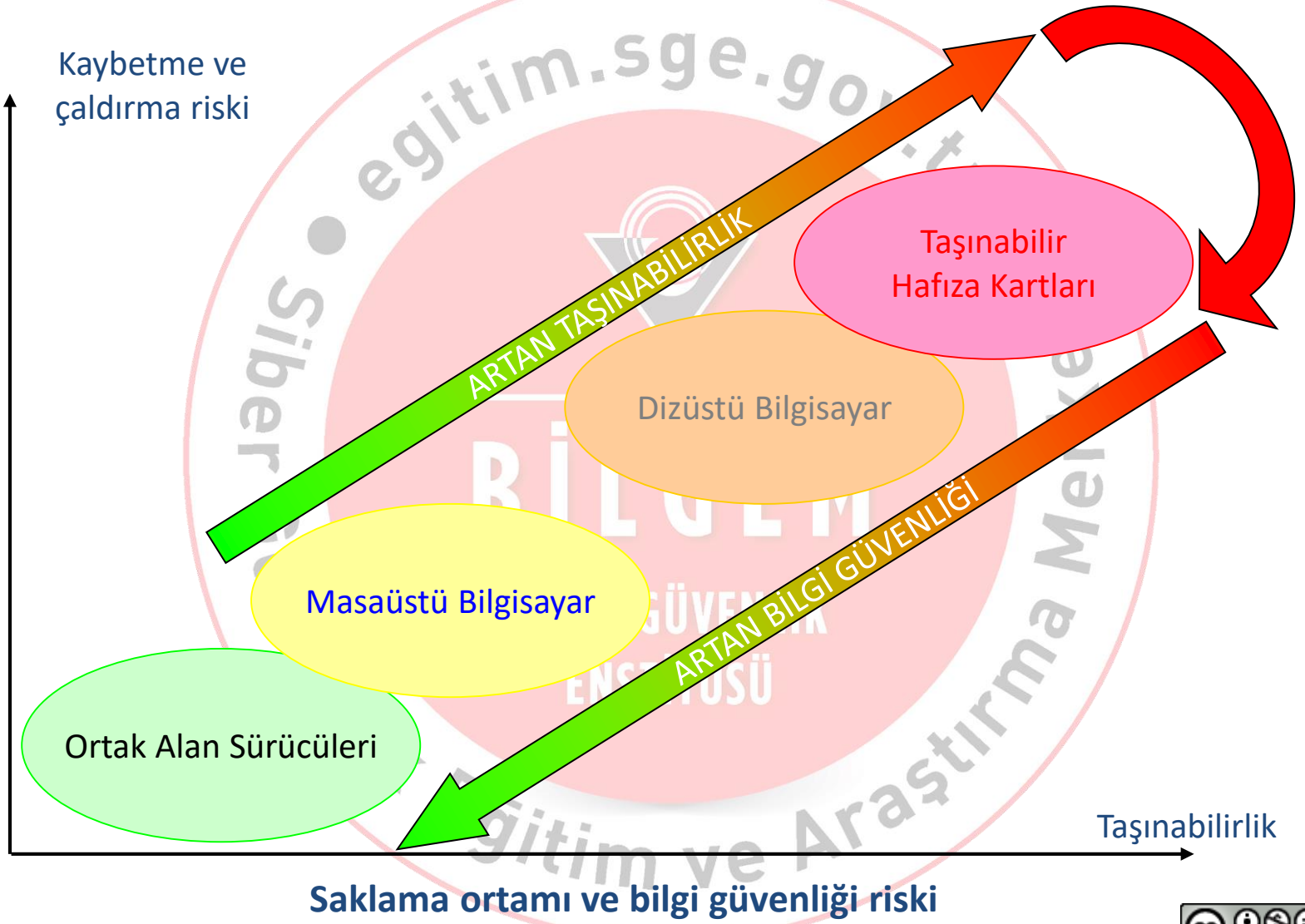
Bir USB bellek, 1 milyon adet kağıtta yer alan bilgi kadar veri içerebilir.

Saklama Ortamlarının Doğru Kullanımı

- Hafıza kartı uygun şekilde kullanılmalıdır!
- *Bilgiyi bir noktadan diğer noktaya taşıma* ✓
- *DEPOLAMA - X*

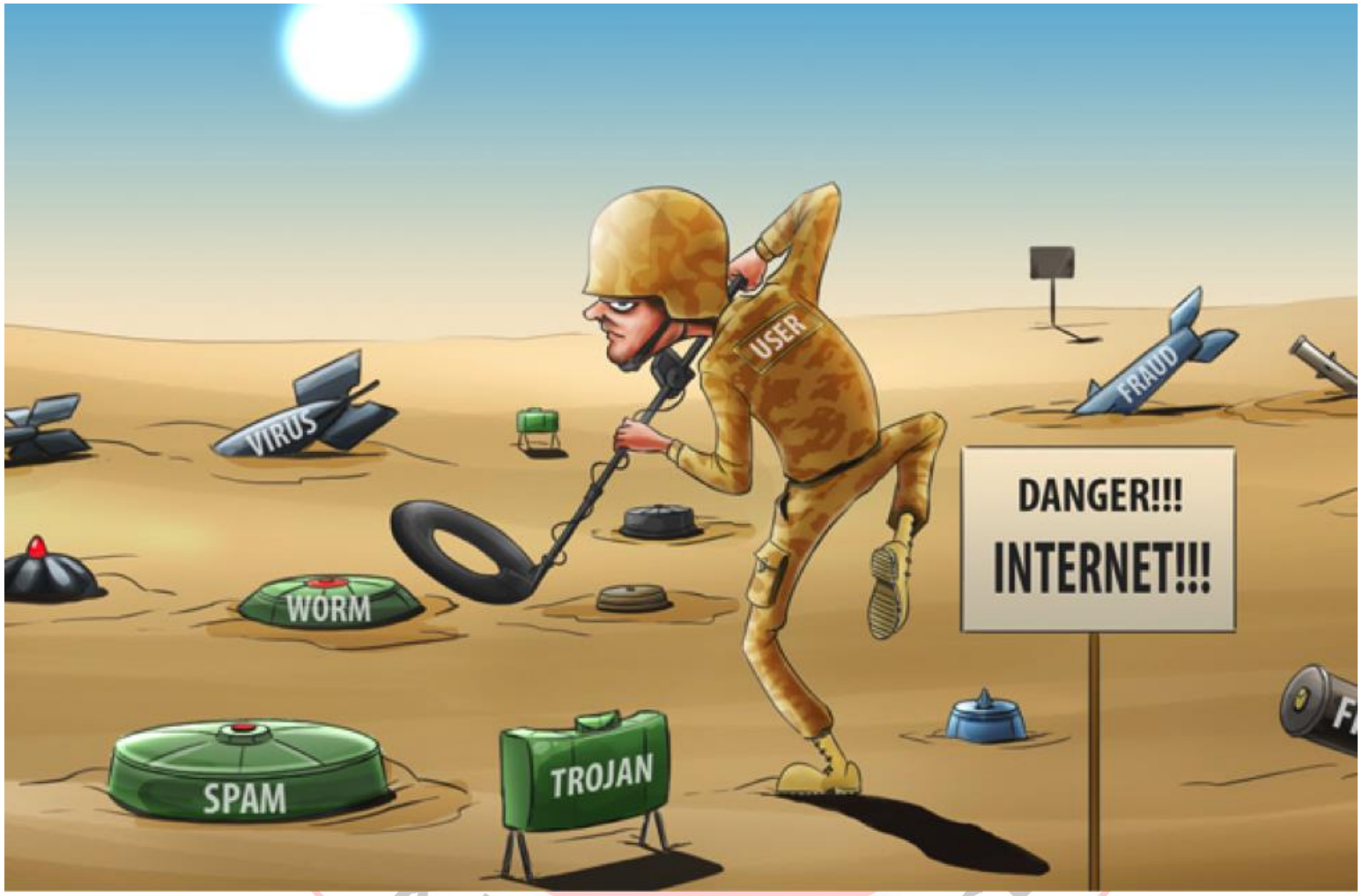
≠

Saklama Ortamlarının Doğru Kullanımı



Zararlı Yazılımlar

Zararlı Yazılımlar - Virüsler



- Virüs koruma programı çalıştırılmalı ve güncellemesi yapılmalıdır.
- Bilgisayardaki «otomatik çalıştır» özelliğinin kapatılması gerekir.
- Uzantısı exe, scr, zip, rar olan dosyalara dikkat!

Ülkelere göre Zararlı Yazılımlar (Bots)

Geography	2015 Bots Rank	2015 Bots %	2014 Bots Rank	2014 Bots %	Annual Change	Change in Number of Attacks Originating from Geography
China	1	46.1%	1	16.5%	+29.7%	+84.0%
United States	2	8.0%	2	16.1%	-8.1%	-67.4%
Taiwan	3	5.8%	3	8.5%	-2.6%	-54.8%
Turkey	4	4.5%	13	2.3%	+2.2%	+29.2%
Italy	5	2.4%	4	5.5%	-3.1%	-71.2%
Hungary	6	2.2%	5	4.9%	-2.6%	-69.7%
Germany	7	2.0%	8	3.1%	-1.1%	-58.0%
Brazil	8	2.0%	6	4.3%	-2.3%	-70.1%
France	9	1.7%	11	2.7%	-1.0%	-57.9%
Spain	10	1.7%	14	2.0%	-0.3%	-44.5%

Kaynak: Internet Security Threat Report, 2016, Symantec

Zararlı Programlar - Truva Atları

What have we learned from history?

Zararlı Programlar - Truva Atları

- Truva atı bilgisayar için yararlı gibi gözüken ve kullanıcının çalıştırması ile aktif olan zararlı yazılımlardır.
- İsmi efsanevi truva atından gelir çünkü çalışmaları için kullanıcının kendi isteği ile truva atını içeri (bilgisayara) alması gerekir.
- Kendilerini virüsler gibi kopyalayamazlar.

Bulaşma Şekilleri

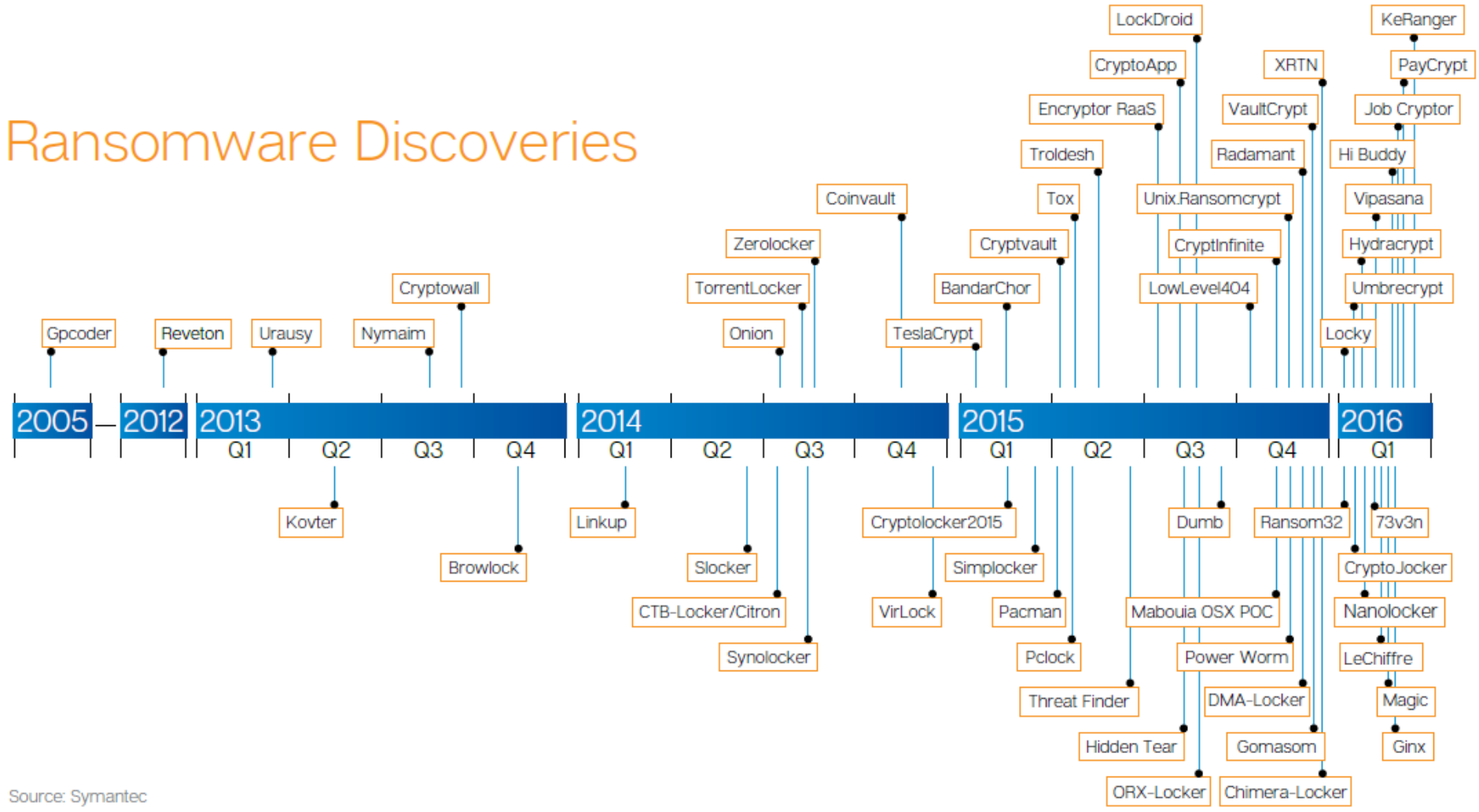
- E-posta eklerini çalıştırarak
- Güvensiz sitelerden indirilen dosyalar ile
- Paylaşım ortamlarındaki dosyalar aracılığı ile

Zararlı Programlar - Fidye Yazılımları

- Bilgisayarınızı kullanmanıza engel olabilen,
- Dosyalarınızın ***ismini değiştirerek*** ya da dosyalarınızı ***şifreleyerek*** kullanmanıza engel olan,
- Şifreyi çözmek için karşılığında para istenen zararlı yazılım türüdür.

mrt@tubitak.gov.tr

Zararlı Programlar - Fidye Yazılımları



Symantec 2016 Internet Security Threat Report

Zararlı Programlar - Şüpheleniyorsanız …

1. Varsa, ilgili kişileri *bilgilendirin*.
2. Güncel bir *antivirüs programı* ile bilgisayarınızı taratın,
   - bulunan virüslerin temizlenmesini,
   - temizlenemiyorsa silinmesini,
   - silinemiyorsa karantinaya alınmasını sağlayın.
3. Güvenlik *duvarı* aktif değilse aktif hale getirin, güncel değilse güncelleyin.
4. İşletim sisteminizin *güncellemelerini* yapın ve ihtiyaç duyulan işletim sistemi *yamalarını* uygulayın.

Sosyal Mühendislik

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 Kavramı

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

- Teknoloji kullanımından çok insanların hile ile kandırılarak bilgi elde edilmesidir.

Sosyal Mühendislik Kavramı

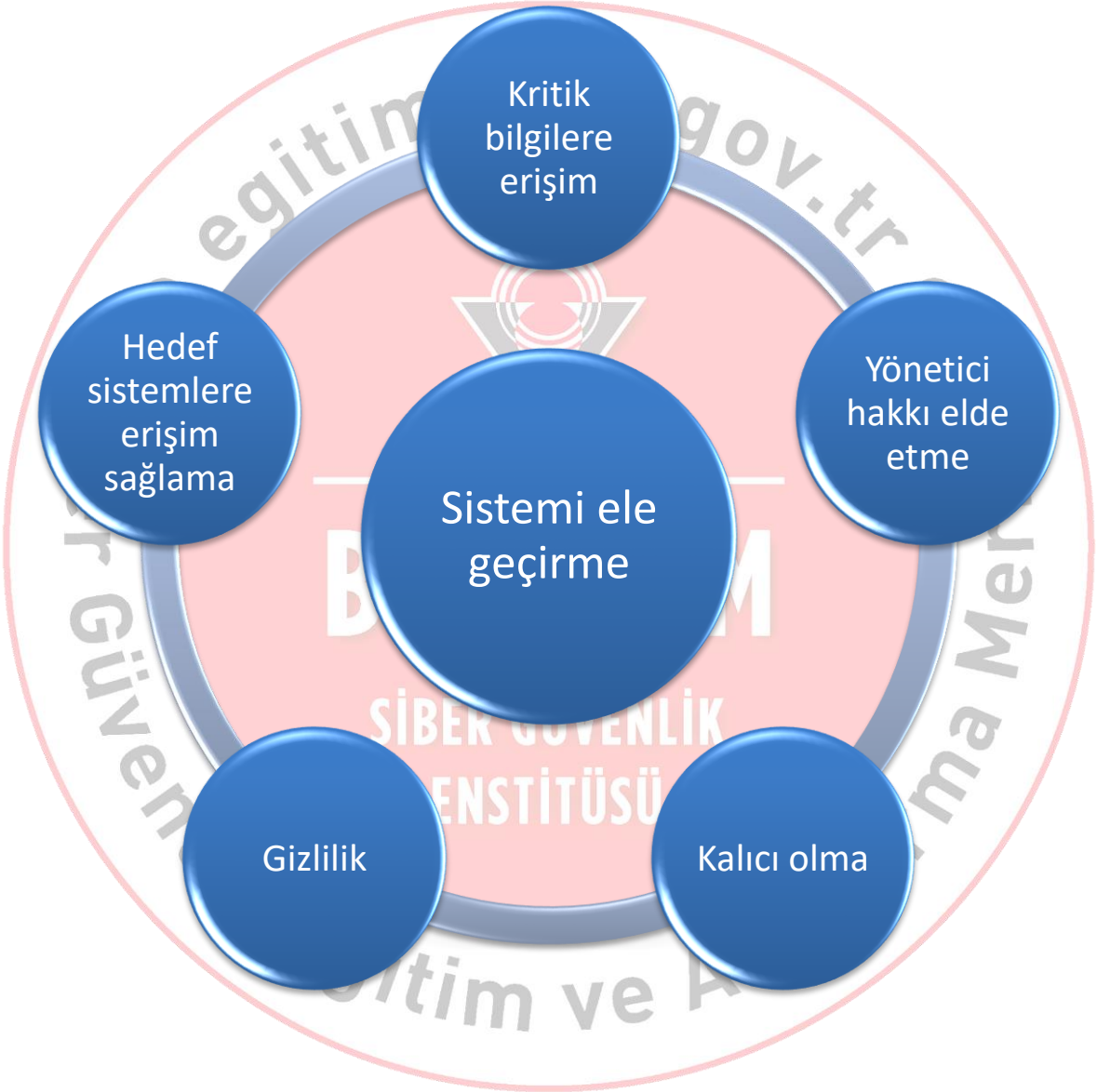
- Çoğu zaman basit dolandırıcılığa çok benzese bile, bu terim genelde bilgi sızdırmak veya bir bilgisayar sistemine sızmak üzere yapılan numaralar için kullanılır.
- Bu durumların büyük çoğunluğunda saldırgan, kurban ile yüz yüze gelmez.
- Kullandığı en büyük silahı, insan zaafiyetleridir.

Bir Sınırı Var mıdır?

İçinde insan olan her süreç bir şekilde **istismar** edilebilir!!

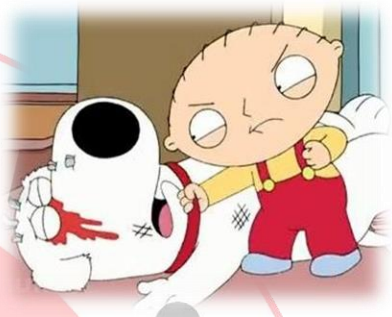
Sosyal Mühendislik Saldırı Teknikleri

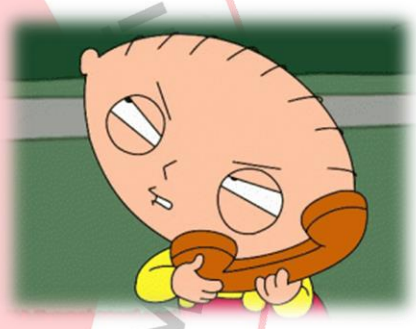
Sosyal Mühendislik Hedefleri

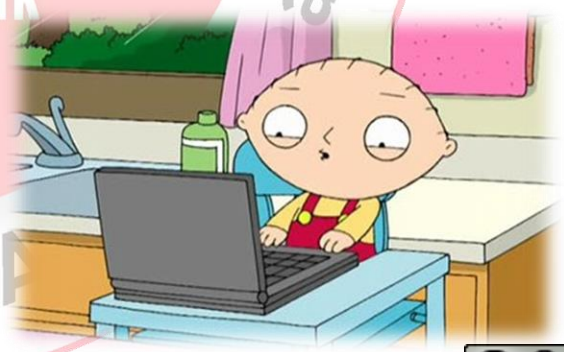


Sosyal Mühendislik Çeşitleri

- Fiziksel sosyal mühendislik
- Telefon ile sosyal mühendislik
- Mail yoluyla sosyal mühendislik







Siber Zorbalık

«Teknolojiyi kullanarak (*internet*, *cep telefonu,..*)

başkasına zarar vermek için tasarlanmış,

kasıtlı ve tekrarlanan *düşmanca davranış*.»

Telefonla Sosyal Mühendislik

- Gerçekçi
- Tedirgin edici
- Güven verici
- Ses tonu

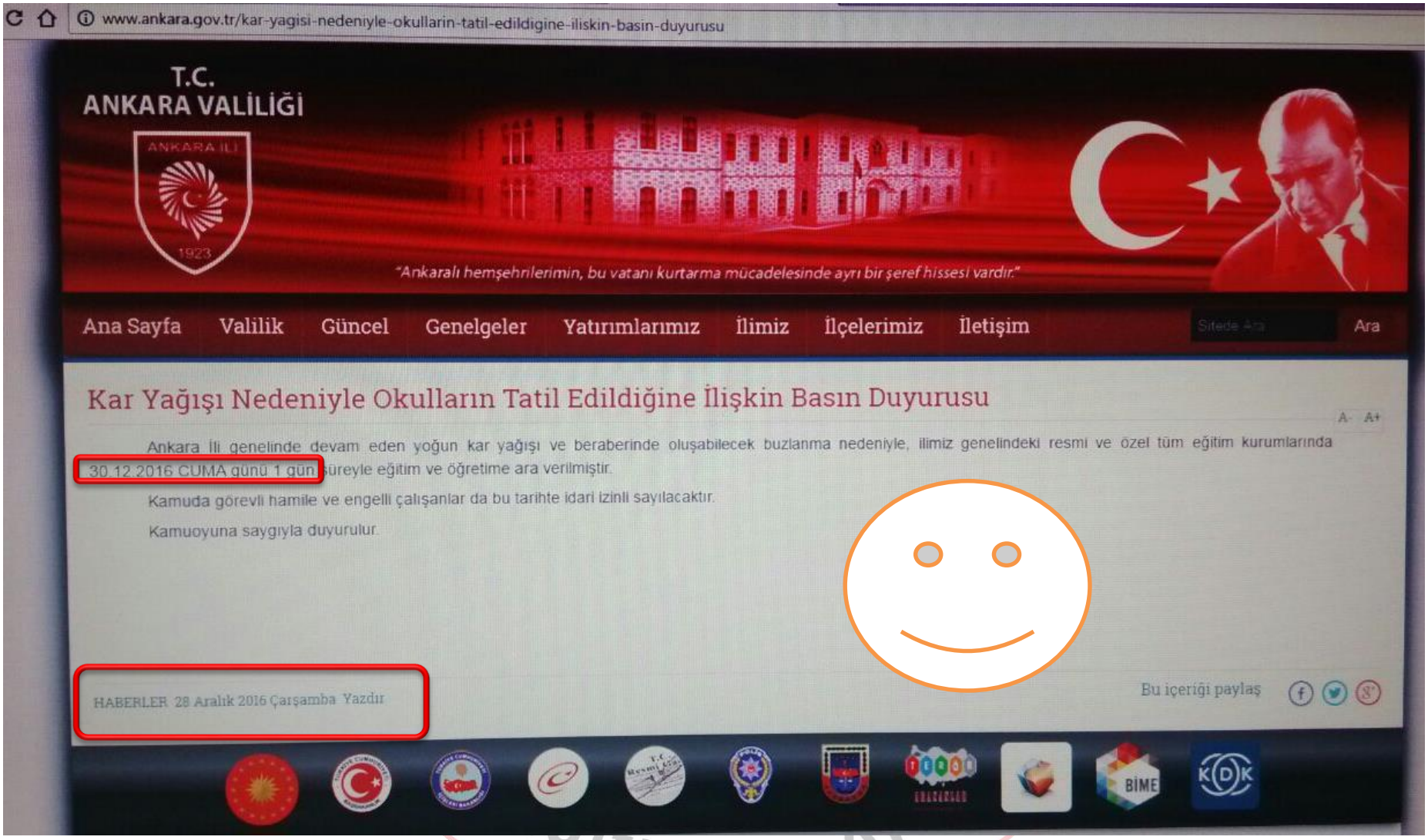
Gerçek Örneklerle Sosyal Mühendislik

Telefon ile oltalama

https://www.youtube.com/watch?v=Kz_soeitDto

Bankalararası Kart Merkezi

29-30 Aralık 2016 Ankara'da Kar Tatili Hikayesi



29 Aralık 2016 saat 20:00'dan önce sosyal medyada yayılan bir resim!

29-30 Aralık 2016 Ankara'da Kar Tatili Hikayesi

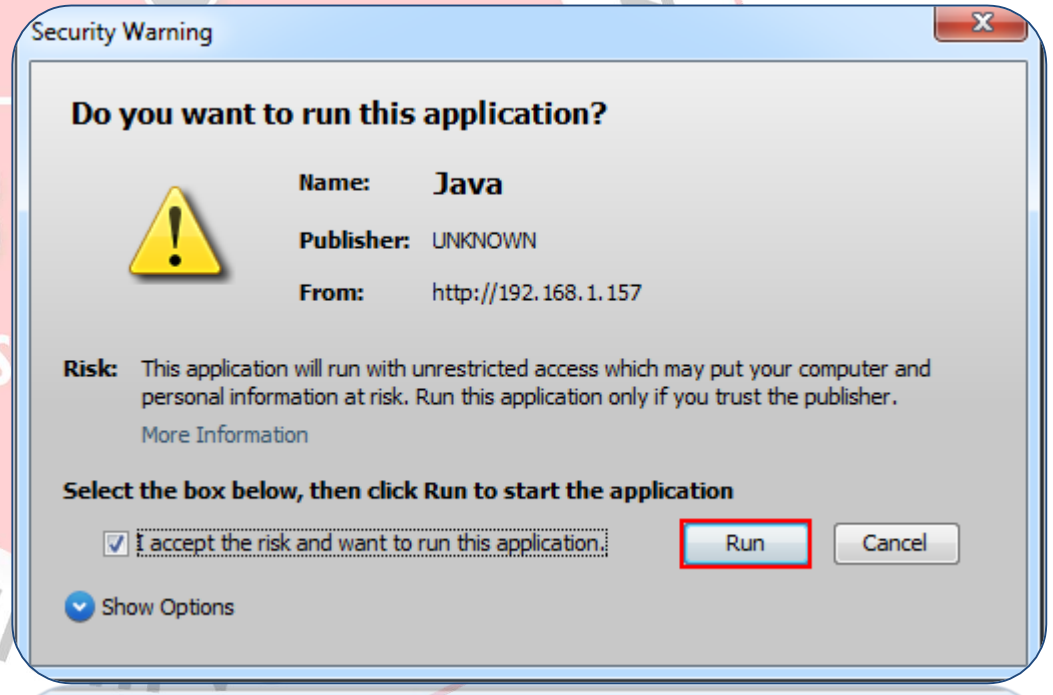
29 Aralık 2016'da 23:00'daki gerçek duyuru!

Senaryolar & Başarı Oranları - Örnek

Telefon Konuşmasıyla Zararlı Siteye Yönlendirme

«Merhaba,
Bilgi İşlem Daire Başkanlığı Sistem Yönetimi Grubundan arıyorum, ismim ……
E-posta sistemimizde kritik güvenlik güncelleştirmesi mevcut ve bazı kullanıcılar bu güncelleştirmeyi almamış. Güncelleştirmeleri almak için söyleyeceğim adrese giriş yapmanız gerekmektedir. »

%90



E-posta Güvenliği

- Bir e-postanın talepte bulunmamış, birçok kişiye birden, zorla gönderilmesi durumunda, bu e-postaya ***istenmeyen e-posta (spam)*** denir.

- ***Taklit (oltalama, phishing) e-postası***, *kimlik bilgilerini çalmak* amacı ile, istenmeyen e-posta veya açılır pencere yoluyla yapılan bir *aldatma yöntemidir*.

Senaryolar & Başarı Oranları - Örnek

Oltalama E-postası Eki

Security Warning Macros have been disabled. Enable Content

BİLİŞİM TEKNOLOJİLERİ DAİRE BAŞKANLIĞI'NDAN

Başkanlık Makamının talimatı doğrultusunda geliştirilen "Bilişim Sistemleri Koruma Kalkanı" yazılımı üzerinden kurumumuz çalışanlarının bilişim sistemleri güvenlik ihlalleri takip edilmektedir. Sistem kayıtlarında yapılan incelemede, kurumsal güvenlik politikamızı ihlal eden kullanıcılar tespit edilmiş olup, ekte listelenmiştir.

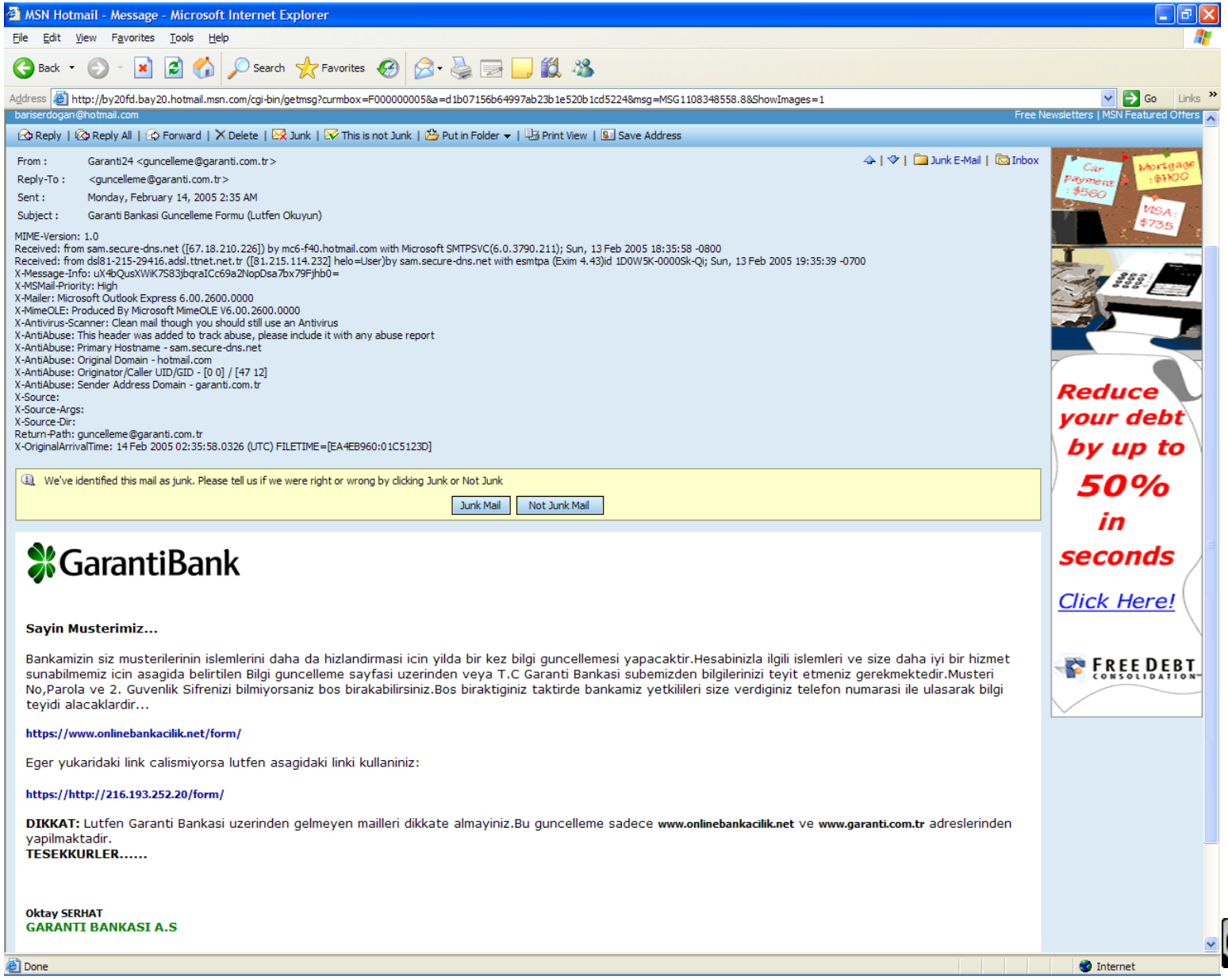
Bilişim sistemleri güvenlik politikasına uyma konusunda daha titiz davranmanız hususunda gereğini önemle rica ederim.

% 116

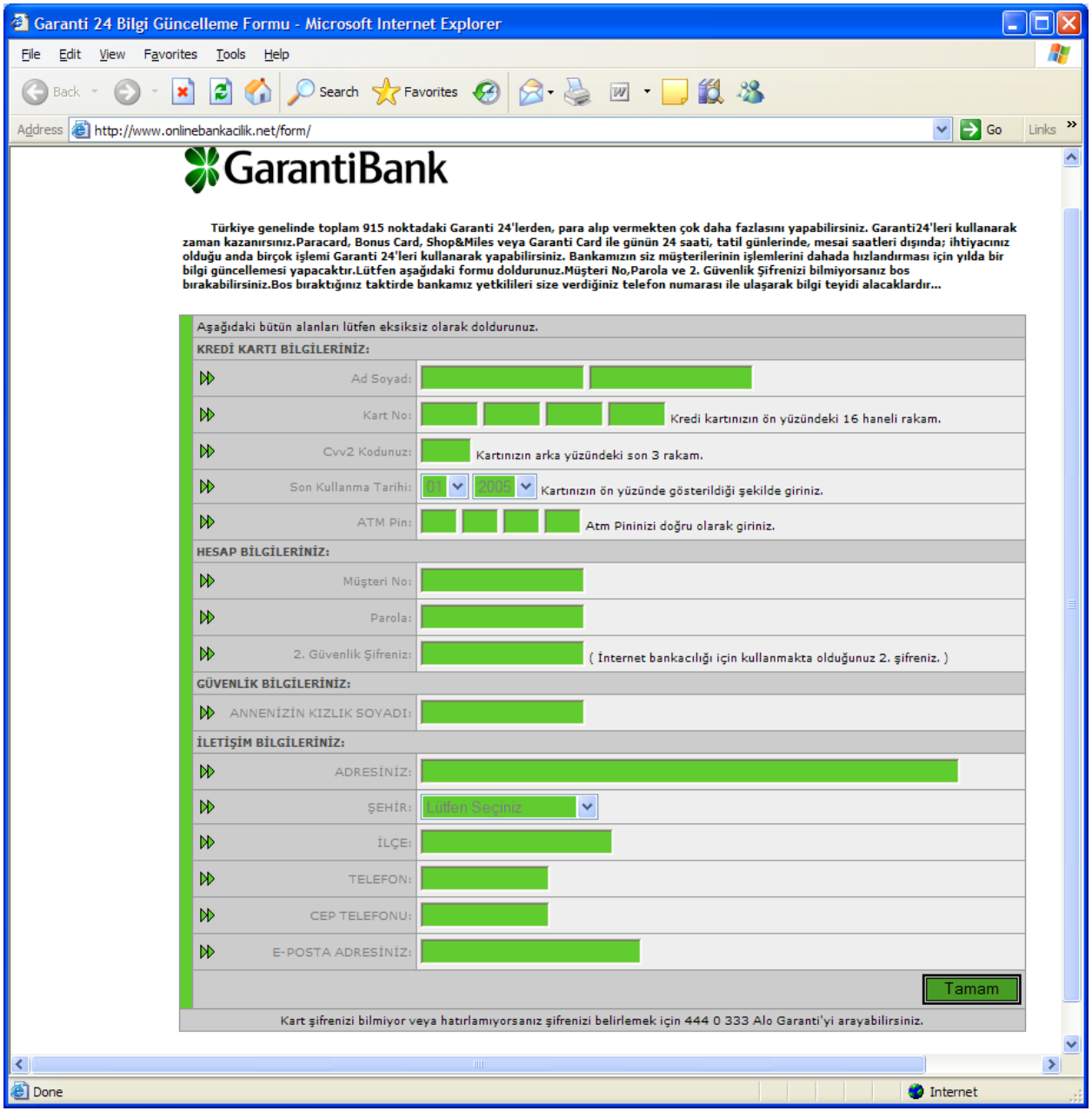
Bilişim Teknolojileri Daire Başkanı

NOT: Kurum personelinin bilişim sistemleri güvenlik ihlallerini gösteren detaylı tablo ekte bulunmaktadır. Tablonun içeriğini düzgün görüntüleyebilmek için makroların etkinleştirilmesi gerekmektedir. Makroları etkinleştirmek için doküman açılınca çıkan güvenlik uyarısının seçenekler kısmından **"Bu içeriği etkinleştir"** uyarısı onaylanmalıdır.

E-posta Güvenliği – Taklit (oltalama) e-posta



E-posta Güvenliği – Taklit (oltalama) e-posta



Sosyal Mühendislik Örnekleri

USB bellekli saat
(19.99$)

Donanımsal keylogger
(59.99$)

USB bellekli çakmak
(39.99$)

Kameralı araba anahtarı
(59.99$)

SD kartı saklayıcısı
(20.99$)

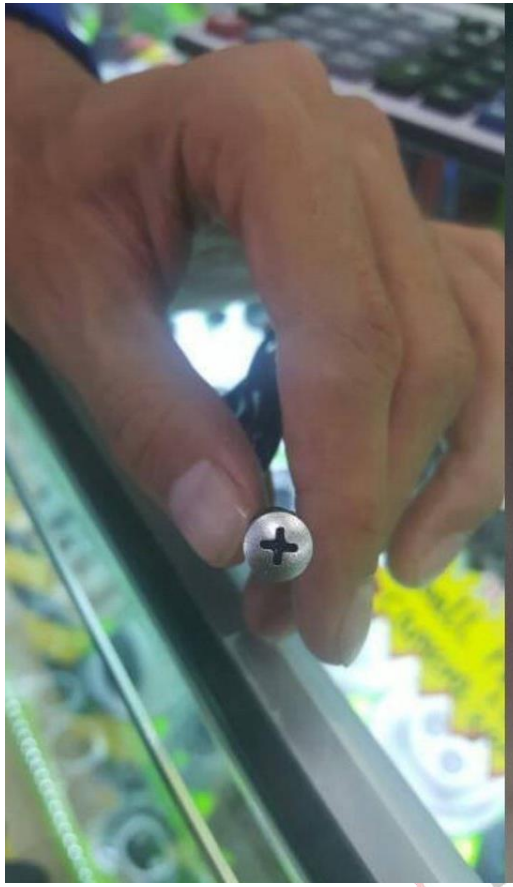
Kameralı kalem
(79.99$)

Kameralı gözlük
(79.99$)

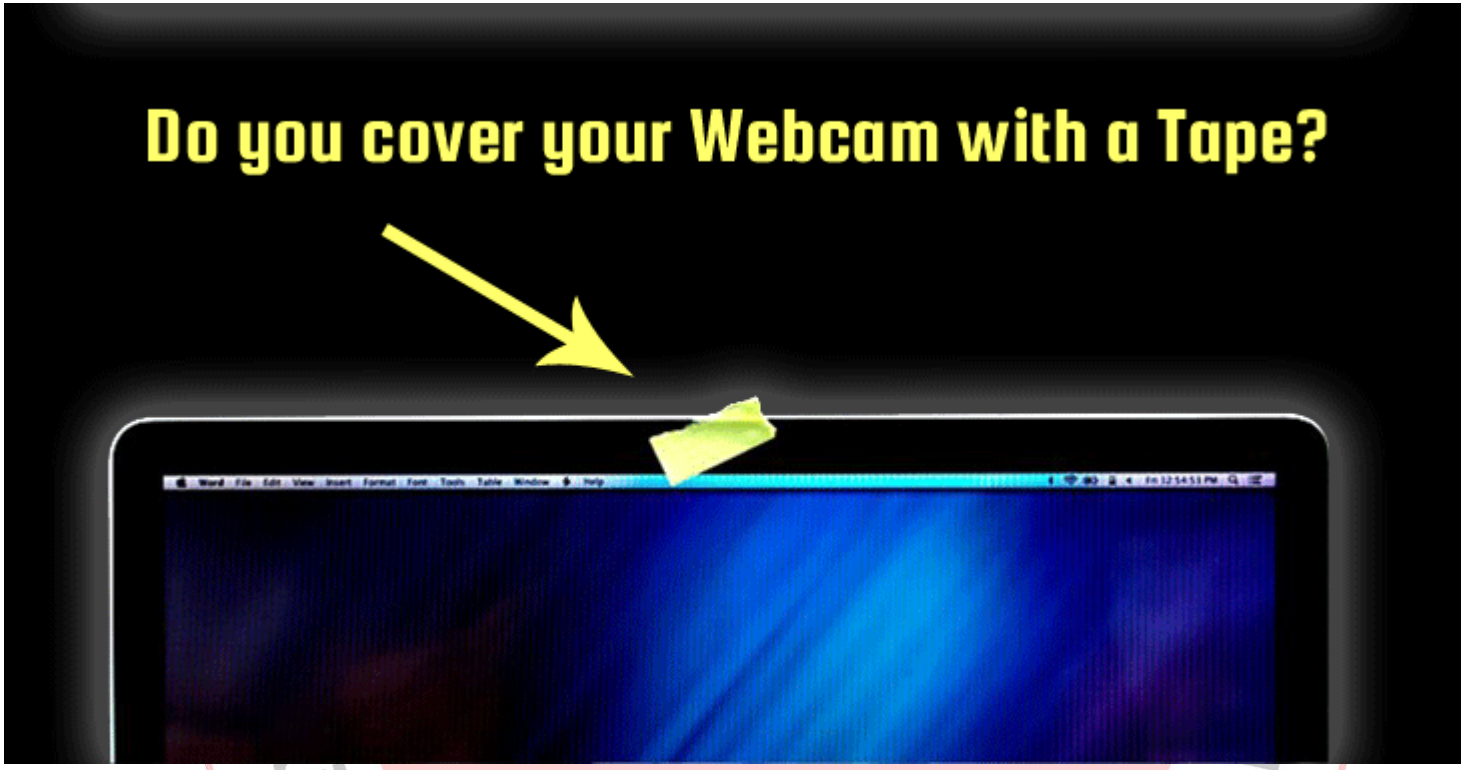
Tarafımızca başka kurumlara yapılan sosyal mühendislik saldırılarından bazı örnekler

1. kayıt: ***2. kayıt:*** ***3. kayıt:***

Sosyal Mühendislik Örnekleri



Sosyal Mühendislik



- Facebook CEO Mark Zuckerberg
- FBI Director James Comey
- Security Consultant Kevin Mitnick
- .....

Yazıcı Kullanımı

- Doküman çıktısının eksik olmadığı kontrol edilmelidir (sayfa ve kopya sayısı bazında)
- Yazıcı hataları ile karşılaşıldığında gönderilen doküman iptal edilmeli ve yanlışlıkla basılmadığı kontrol edilmelidir.
- Çıktının yazıcıda basılması süresinde dokümanın başında bulunulmalıdır.

- Kurumun çöplerini attığı yerleri karıştırabilirler.
- Bu nedenle çöplerinize kurumsal bilgi içeren kağıtlar atmayınız.

Sosyal Mühendislik - Alınacak Tedbirler

- Taşıdığınız, işlediğiniz bilgilerin kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket edin.
- Arkadaşlarınızla paylaştığınız bilgileri seçerken dikkat edin.
- Özellikle telefonda, e-posta veya sohbet yoluyla yapılan haberleşmelerde parola gibi özel bilgilerinizi kimseye söylemeyin.
- Parola kişiye özel bilgidir, sistem yöneticinize bile telefonda veya e-posta ile parolanızı söylemeyin. Sistem yöneticisi gerekli işlemi parolanıza ihtiyaç duymadan da yapacaktır.

Kitap Önerisi

Aldatma Sanatı, Kevin D. Mitnick, William L. Simon, ODTÜ Geliştirme Vakfı Yayıncılık, Şubat 2009.

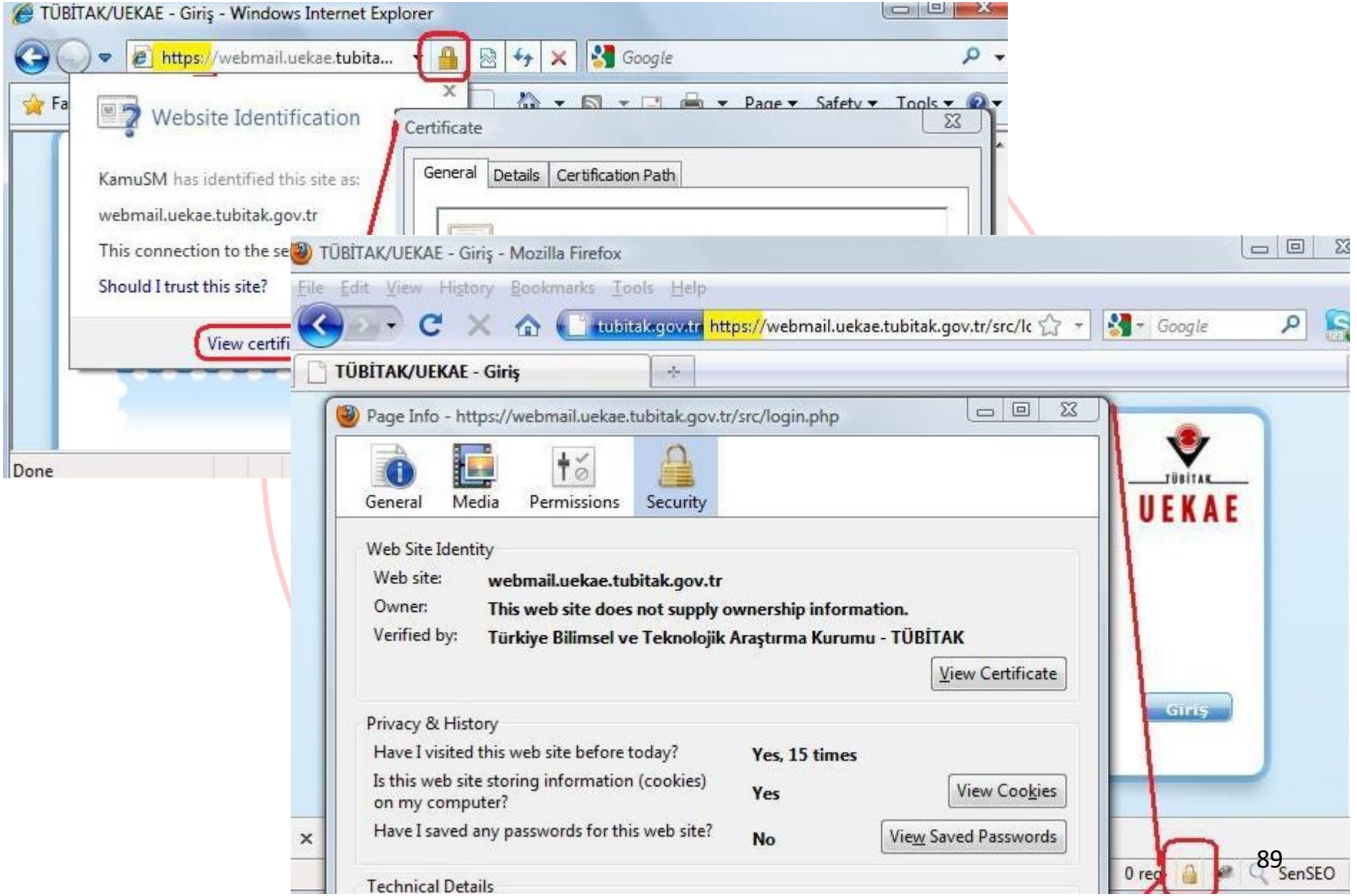
Web ve E-posta Güvenliği

Web Güvenliği

Bizler nasıl Türkçe, İngilizce gibi dilleri kullanarak anlaşıyorsak, internette de *http*, *ftp*, *https* gibi isimlendirilen protokoller ile veri alışverişi sağlanır.

Peki bu protokoller ile sağlanan veri alışverişi ne kadar güvenlidir?

Web Güvenliği



Web Güvenliği

HTTP/FTP Erişimlerinde Nelere Dikkat Etmeli?

- Şifrenizin değişmesi gerektiğini belirten web sayfaları ya da e-posta mesajlarına,

- çok fazla bilinmeyen,
- bahis siteleri,
- pornografik içerik sunan,
- korsan yazılım indirilen

siteler gibi bilgisayar virüsü ve tehlikeli yazılımları davet eden sitelere dikkat edilmelidir.

Ülkelere göre Zararlı Yazılımlar (Spam)

Geography	2015 Spam Rank	2015 Spam %	2014 Spam Rank	2014 Spam %	Annual Change	Change in Number of Attacks Originating from Geography
China	1	47.4%	11	3.4%	+44.0%	+255.0%
United States	2	8.5%	9	3.9%	+4.6%	-45.1%
Taiwan	3	5.2%	10	3.6%	+1.7%	-63.0%
Turkey	4	4.9%	40	0.5%	+4.5%	+176.1%
Italy	5	2.3%	12	3.2%	-0.9%	-81.8%
Hungary	6	2.2%	52	0.2%	+2.0%	+250.6%
Germany	7	2.0%	5	5.8%	-3.8%	-91.3%
Brazil	8	1.9%	13	2.1%	-0.2%	-77.1%
France	9	1.7%	41	0.4%	+1.2%	-5.5%
Canada	10	1.7%	42	0.4%	+1.3%	+6.3%

Kaynak: Internet Security Threat Report, 2016, Symantec

E-posta Güvenliği – oltalama e-postalara karşı

- *Kişisel ve mali bilgilerini* tanıdığın kişiler dâhil hiç kimseye *e-posta yoluyla göndermemek*.
- E-posta *mesajlarındaki internet bağlantılarına* tıklamamak.
- Düzenli olarak kredi kart hesap özeti, banka bildirimleri gibi *bilgilendirme dokümanlarını gözden geçirmek*.
- Zararlı programlara karşı korunma programları (*Anti-virus, anti-spyware, güvenlik duvarı*) gibi güvenlik yazılımları kullanmak ve bu programları sık sık güncellemek.

E-posta Güvenliği – İstenmeyen E-posta Örneği

E-posta'nın kimden bölümündeki adres yanlış.

E-posta'nın kime bölümündeki adres E-postanın geldiği kişiye ait değil.

İlgi çekici bir konu.

Genellikle her spam E-postada olan üyelik sildirme bölümü.

E-posta Güvenliği – istenmeyen e-postalara karşı

- E-posta adresini herkese açık yerlerde yayınlamamak, gerekirse, *adresi maskeleyerek* yayınlamak.
- Birçok kişiye veya gruba e-posta gönderirken kişilerin adreslerini *gizli karbon kopya (BCC) bölümüne* yazmak.
- İstenmeyen e-postalara hiç bir şekilde *cevap yazmamak.*
- Kullanım amacına göre *farklı e-posta adresleri* kullanmak.
- Bilmediğiniz haber ve e-posta gruplarına üye olmayınız.

E-posta Güvenliği – istenmeyen e-postalara karşı

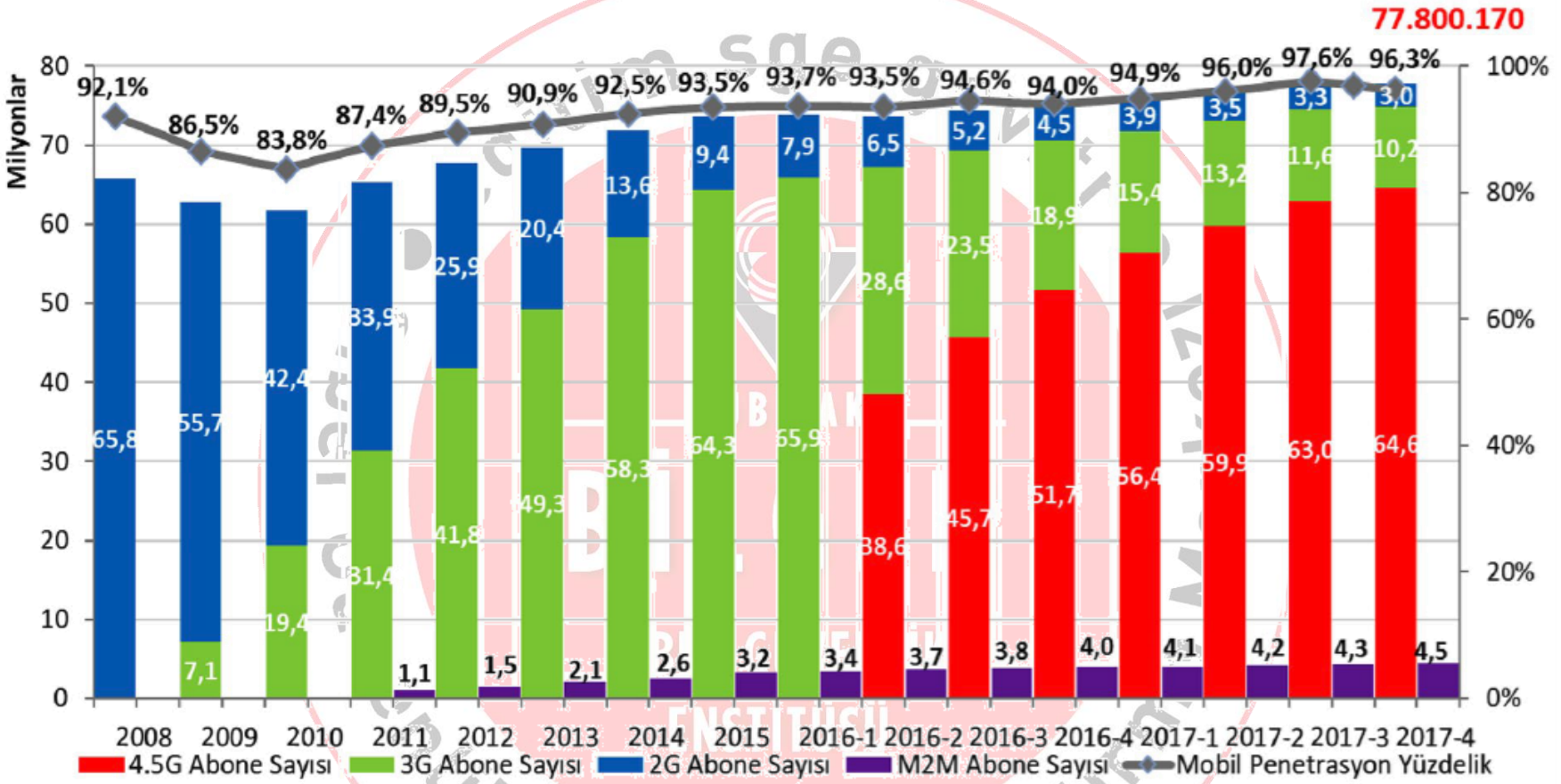
- Kişisel dosyaları fıkra, karikatür, ses dosyası vs. kurumun size tahsis ettiği ***kurumsal e-posta*** adresinizden yollamayınız.
- Çoğu istenmeyen e-posta sonunda bulunan üyelik sildirme formu ***kullanılmamalıdır***.

Mobil Cihaz Güvenliği

Bilgisayar, Akıllı Telefon, Tablet

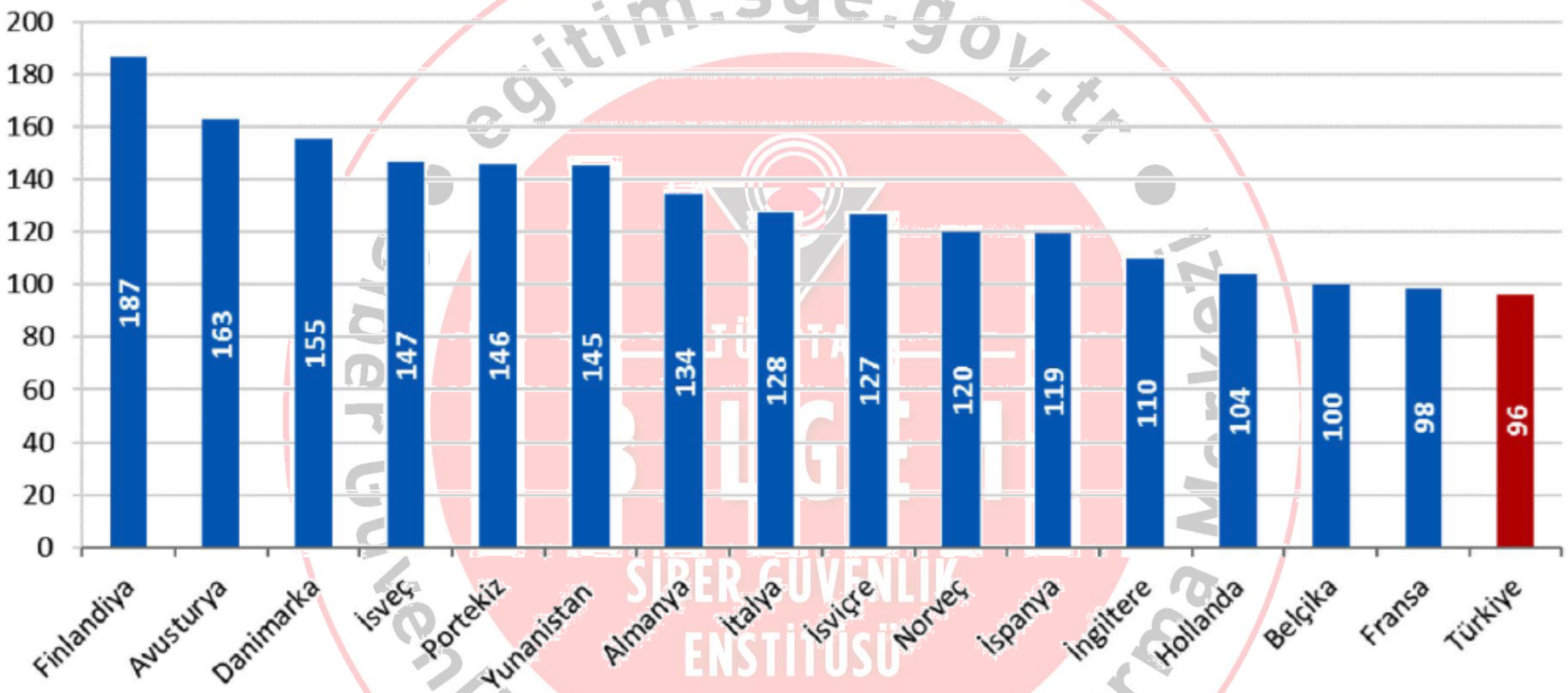
- 2000 yılında dünyada muhafaza edilen bilginin sadece dörtte biri dijitalken: **%25**
- 2013'te dijital olmayan verilerin oranı yüzde 2: **%98**
- 2016 yılında **5** bağlantıdan **4**'ü mobil platformlardan

Türkiye'deki Toplam Mobil Abone Sayısı ve Nüfusa Göre Penetrasyon



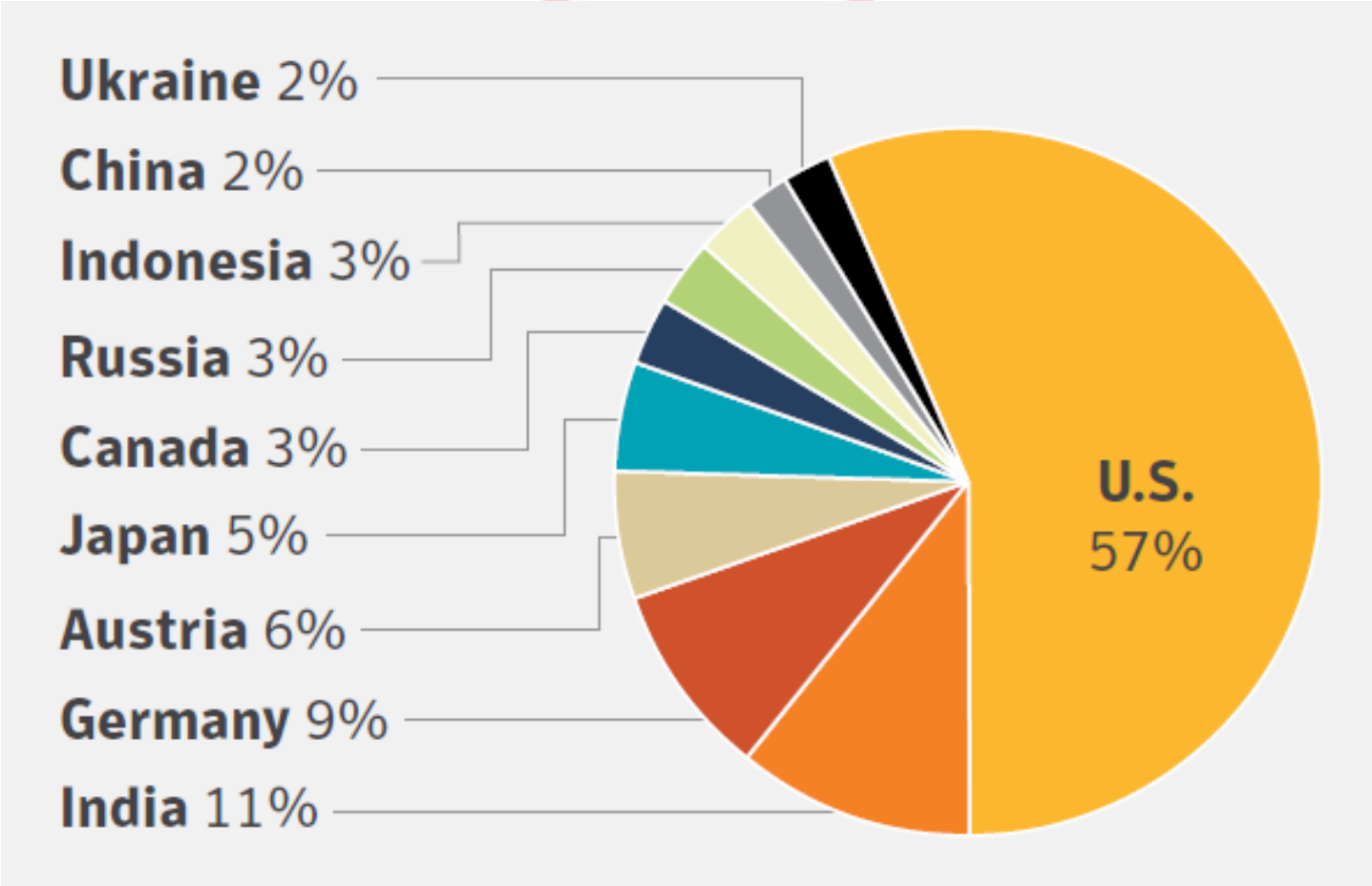
BTK Pazar Verileri Raporu, 2017-4.
https://www.btk.gov.tr/uploads/pages/2017-q4.pdf

Türkiye ve Bazı Avrupa Ülkelerinin Mobil Penetrasyon Oranları, %



BTK Pazar Verileri Raporu, 2017-4.
https://www.btk.gov.tr/uploads/pages/2017-q4.pdf

Mobil Zararlı Yazılımların Ülkelere Göre Dağılımı

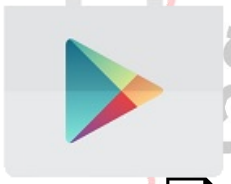


Internet Security Threat Report – ISTR Volume 23 - 2018 - Symantec

Akıllı Telefonlarda Mahremiyet ve Gizlilik

https://m.youtube.com/watch?feature=youtu.be&v=rcYgCy0VYMQ

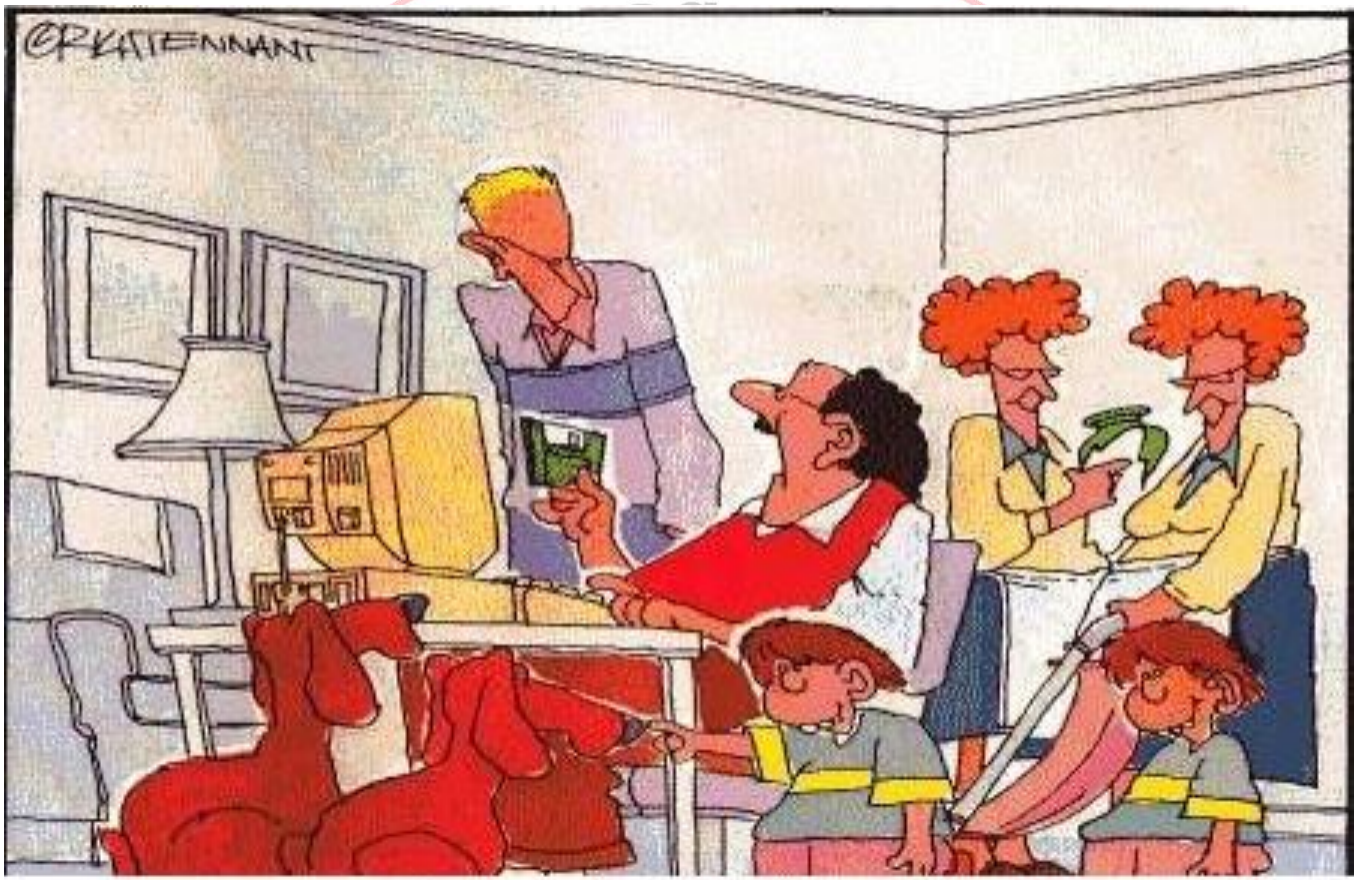
Mobil Cihazlarda Güvenlik



- ❑ Standart bilgisayarlara göre çok daha fazla güvenlik!
- ❑ Mutlaka parola, parmak izi, yüz tanıma vb. kilitleme!
- ❑ Kullanılmadığı zamanlarda Wi-Fi kapalı olmalı!
- ❑ Uygulamalar güvenilir ortamlardan yüklenmeli!
- ❑ Uygulamanın talep ettiği izinler dikkatlice incelenmeli!
- ❑ İşletim sistemleri ve uygulamalar sürekli güncel tutulmalı!
- ❑ Cihazların satılmadan, teknik servise teslim edilmeden veya bir başkasına verilmeden önce içeriği güvenli bir şekilde silinmelidir.

Yedekleme

Yedekleme



Ben herşeyimi back-up'larım da...

Yedekleme

- Yedekleme + yedekten geri dönme prosedüre bağlanmalıdır.
- Gizli bilginin yedeği de gizlidir.
- Yedekler asıl bilgiden uzakta saklanmalıdır.
- *İnsan kaynağının yedeklenmesi?*

Yedekleme

Bir kurum çalışanı nelere dikkat etmeli?

- Kurumun yedekten geri dönme prosedürlerini öğrenmek.
- Kurumun yedekleme dönem ve zamanlarını bilmek.
- Kurumsal olarak otomatik yedeklenen klasörleri bilmek.
- Kurumsal bilgileri veya yedeklenmesi gereken tüm dokümanları yedeği alınan klasör altına kaydetmek.

Bilinçlendirme Web Siteleri

www.bilgimikoruyorum.org.tr

TÜBİTAK

Ana Sayfa | Hakkımızda | TÜBİTAK | BİLGEM

BİLGEM | Bilgimi Koruyorum

Google™ Özel Arama | Ara

Bilgimi Koruyorum ▸ Ana Sayfa

B!resi biTgileranizi demiftirse

Öeler olapilix?
Ne hi$$ebersiniz?
Nz yaşarsıMız?

Bilgi güvenliği; kendimizi geliştirmekle, öğrendiklerimizi uygulamakla ve öğrendiklerimizi yakınlarımızla paylaşmakla sorumlu olduğumuz bir konu. **Güvenlik tedbirleri almadan bilişim teknolojilerini kullanmak** günümüzde "*inanılmaz bir risk alıyorsunuz*" anlamına geldi. Kısacası bu konudan uzak durmak istesek bile o bizim yakamızı bırakacak gibi görünmüyor.

Öyleyse **en iyisi öğrenmek**. Aslında günlük yaşamımızdan hiç yabancısı olmadığımız bir çok kavram ve yaklaşım içeren bu konuyu, Çağlar Bey ve arkadaşlarının dünyasında geçen olaylarla irdelemeye, bilişim dünyasında bilinçli hareket etmeye hoş geldiniz.

Bilgi güvenliği: Nedenleri / Sorumluluklar

Bilgisayara giriş güvenliği

Parola güvenliği

Konu Listesi / Menü

- Bilgimi Koruyorum
- Bilgi Güvenliği
- Bilgisayar ve Erişim Güvenliği
- Tehditler ve Korunma Yöntemleri
- Internet ve Ağ Güvenliği

Sözlük

TÜBİTAK | BİLGEM

◂ Bilgimi Koruyorum

Eğitime Başlarken (Öneriler) ▸

Evimi Koruyorum

Bilgimi Koruyorum

www.bilgiguvenligi.gov.tr

TÜBİTAK

TÜBİTAK BİLGEM

Ulusal Bilgi Güvenliği Kapısı

Hakkımızda | İletişim/Bilgi Edinme | Sıkça Sorulan Sorular | Yorumlarınız | RSS | Arama

Bilgi için: bilgi at bilgiguvenligi gov tr

Ana Menü

- Anasayfa
- Etkinlikler
- Güvenlik Bildirileri
- Teknik Yazılar
- Kılavuzlar
- Herkes İçin Güvenlik
- Raporlar
- Duyurular
- Terimler Sözlüğü
- Site İçerisinde Arama
- İçerik Arşivi
- Ortak Kriterler

Ulusal Bilgi Güvenliği Kapısı'na yazılarınızla katkıda bulunmak ister misiniz?

Kullanıcı Adı

Parola

Güncel Açıklıklar

- Oracle Kritik Yama Güncellemesi – Temmuz 20...
- Open SSL Çoklu Güvenlik Açıklıkları
- Linux Çekirdeği "n_tty.c" Bellek Bozulması ...
- Internet Explorer Uzaktan Kod Çalıştırma Gü...
- OpenSSL TLS Heartbeat Eklentisi Bilgi İfşas...

Duyurular

Siber Güvenlik Yaz Okulu 2014

p 2012 ve 2013 yıllarında Siber Güvenlik Yaz Kampı adıyla

Akustik Gizli Kanal Ağlar

Furkan ÇALIŞKAN, TÜBİTAK BİLGEM KAMUSM
13.08.2014

Gizli iletişim kanalı olarak Türkçe'ye çevrilebilecek **'covert channel'** kavramı bir sistemin herhangi bir değerinin modüle edilerek o değer üzerinden veri iletmek anlamında kullanılmaktadır. Örneğin kötü niyetli bir uygulama CPU'yu belirli aralıklarda aşırı meşgul edip aynı süre miktarı kadar da belirli aralıklarda boşta bırakıyorsa,...

Devamını oku...

Türkiye'de İletişim Hizmetleri

Tolga MATARACIOĞLU, TÜBİTAK BİLGEM
06.08.2014

İletişim hizmetlerini sınıflarken, sektörün düzenleyici/denetleyici kurumu olan BTK'nın verilerinden faydalanılmıştır. BTK Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı tarafından üç ayda bir yayınlanan **"Türkiye Elektronik Haberleşme Sektörü – Üç Aylık Pazar Verileri Raporu 2012 Yılı 3. Çeyrek"**...

Devamını oku...

Temel Seviye Güvenlik Belgelendirmesi (TSGB)

Koray Atsan, TÜRKSAT A.Ş.
31.07.2014

Bilgi güvenliği standardları incelendiğinde **ISO/IEC 27001** serisi Bilgi Güvenliği Yönetim Sistemi standardları ile **ISO/IEC 15408** Ortak Kriterler standardları ön plana çıkar. Bu standardlardan ilki bilgi teknolojisi süreçlerinde güvenliği yönetimsel açıdan ele alırken ikincisi ise ürün temelli bir belgelendirme yaklaşımı sağlar....

Devamını oku...

Herkes İçin Güvenlik Bölümü

Daha çok ofis ve ev kullanıcılarının bilgi güvenliği ihtiyaçlarına yönelik teknik yazı ve kılavuz dokümanların yer alacağı **Herkes İçin Güvenlik Bölümü**'ne **buradan** ulaşabilirsiniz.

Anket

Ulusal siber güvenliğin sağlanmasında en öncelikli gördüğünüz konu hangisidir?

- Kritik altyapıların (enerji, su, finans vb.) korunmasına yönelik tedbirlerin alınması
- Bilgi güvenliği uzmanı yetiştirilmesi, eğitim programlarının hazırlanması
- Toplumda bilgi güvenliği farkındalığının oluşturulması
- Milli siber güvenlik ar-ge projelerinin teşvik edilmesi ve kullanımı
- Ülkedeki siber güvenlik yönetim organizasyonun kurulması ve yönetim sürecinin işletilmesi

www.guvenliweb.org.tr

www.guvenlicocuk.org.tr

guvenliinternet.org

www.stopthinkconnect.org

www.saferinternet.org.uk

Bilinçlendirme Posterleri

Poster – SGE


* * * * * * * *
PAROLANI DEĞİŞTİRMEK İÇİN SADECE
6
SAATİN VAR!
{ 8 karakterli bir parola 6 saatten az sürede kırılabilir }
BİLGEM SGE
Siber Güvenlik Enstitüsü
www.bilgiguvenligi.gov.tr
www.bilgimikoruyorum.org.tr
www.bilgem.tubitak.gov.tr

Poster – SGE


KURUM_AL
GÜV__LİK
SEN'siz Olmaz!
BİLGEM SGE
Siber Güvenlik Enstitüsü
www.bilgiguvenligi.gov.tr
www.bilgimikoruyorum.org.tr
www.bilgem.tubitak.gov.tr

Poster - Sosyal Ağlar ve Siber Zorbalık

STOPTHINKCONNECT.ORG

Poster - Internet

Poster - Sosyal Ağlar ve Siber Zorbalık

Poster - Sosyal Ağlar ve Siber Zorbalık

www.educause.edu

Bilgisayar Korsanlarından 7 Güvenlik Önerisi

1. Akıllı telefonunuzda Wifi ve Bluetooth kapalı olsun!
2. İki aşamalı kimlik doğrulama kullanın!
3. Güçlü parola stratejisi!
4. Her zaman HTTPS tercih edin!
5. Evde kablosuz ağınızı koruyun!
6. Evde kablosuz ağınızı (SSID) gizlemeyin!
7. Internete bağlı cihaz almadan önce 2 kere düşünün!

Son Söz

- Kendimizi, ailemizi, okulumuzu, veya kurumumuzu korumak için
- Bilgilerimizi ve belgelerimizi korumak için
- Maddi kayıpları önlemek için
- Zaman ve efor kaybının önlemek için
- Toplumdaki imajımızı korumak için

Unutmayın!
Bir Bilgi Güvenliği Farkındalığı Eğitimi, sizi bir şemsiyenin yağmurdan koruyabildiği kadar korur!

TÜBİTAK

Teşekkürler