



Kullanıcı Güvenliği Eğitimi

TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü



Bu doküman, alıntı vererek kullanılabilir ya da paylaşılabılır ancak değiştirilemez ve ticari amaçla kullanılamaz. Detaylı bilgiye <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.tr> bağlantısından erişebilirsiniz.

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

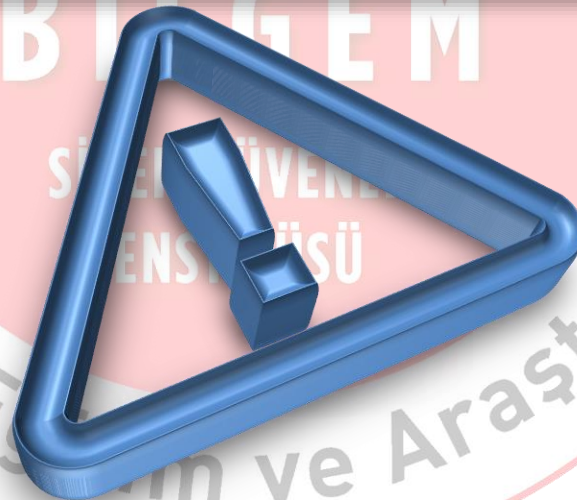
Yedekleme

Amaç

SİBER GÜVENLİK
ENSTİTÜSÜ

“Yazılı ve elektronik ortamdaki kurumsal bilgiyi korumak”

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



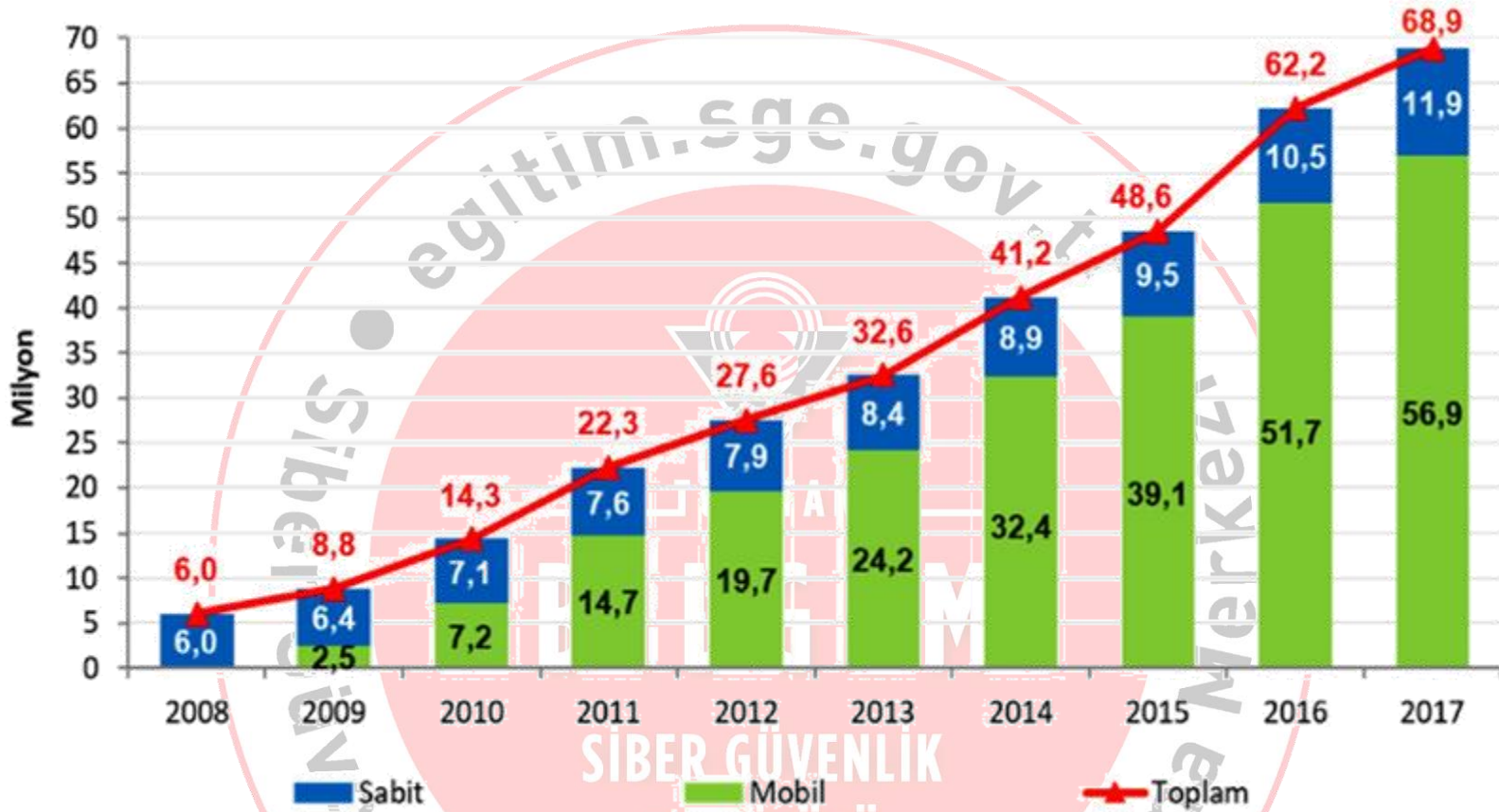
Ya da, kurum olağan işleyişini gerçekleştiremez ve itibar kaybeder.





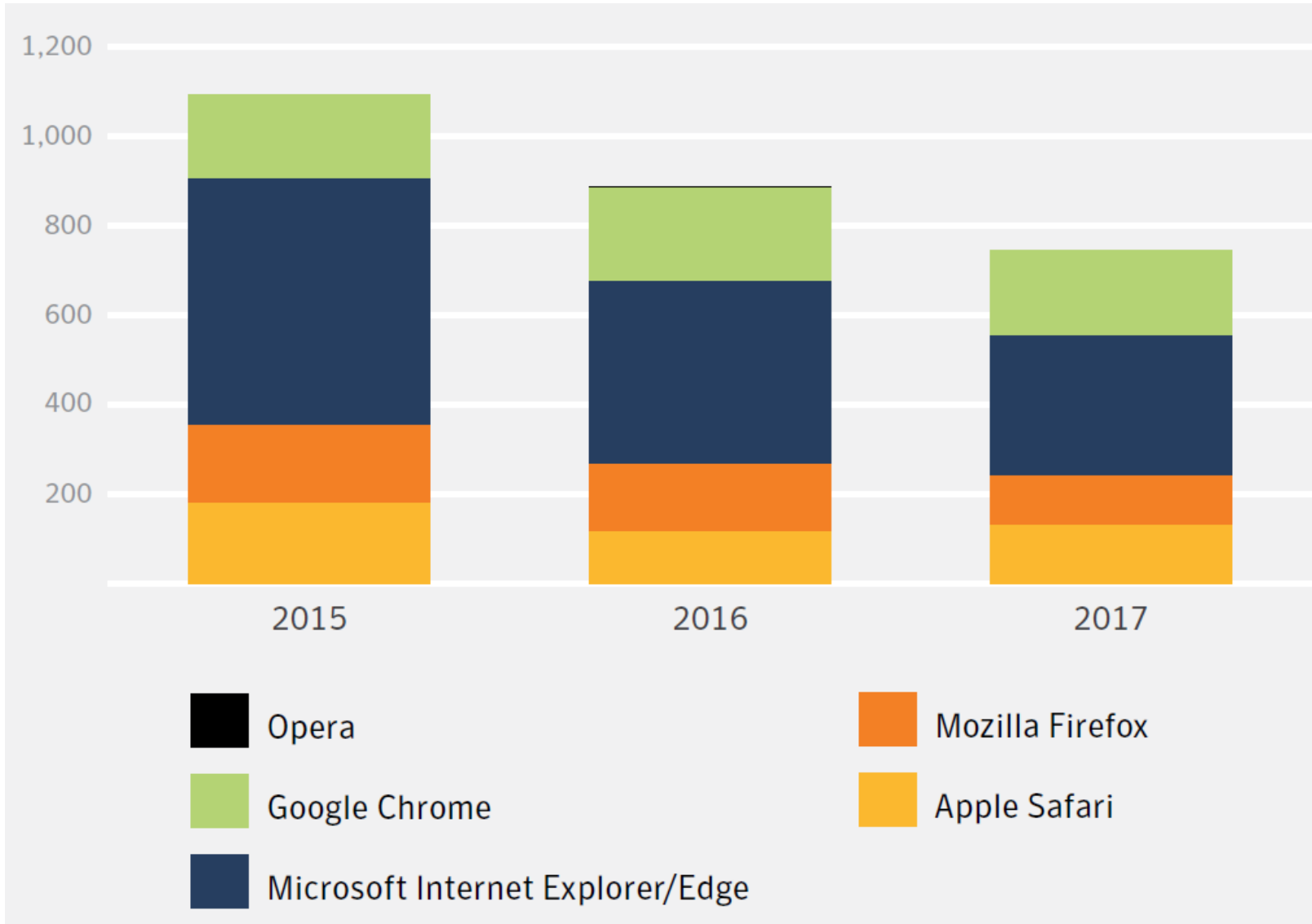
- Bilgi güvenliği, kurumsal bilginin
 - **Gizliliğinin,**
 - Bütünlüğünün ve
 - Erişilebilirliğininsağlanmasıdır.

Siber Uzay (Internet)



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

İnternet Tarayıcılarıdaki Açıklıklar



ABD’de gerekleŖen en kapsamlı DDoS Saldırısı



- 20 Ekim 2016 tarihinde gerekleŖtiriliyor.
- 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 gerekleřen en kapsamlı DDoS Saldırısı

- Ayrıca ABD hükümetine ait kurum ve kuruluşların sitelerinin de öktüğü 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.
- arşamba günü Mirai zararlı yazılımının yaklaşık 500.000 cihaza bulaştığı ifade ediliyor.

1 Tbps DDoS Attack

Powered By 150,000 Hacked IoT Devices



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 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 Saldırıları 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

ğitim ve A



Sorumluluk

SİBER GÜVENLİK
ENSTİTÜSÜ

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



Bunu biliyor muydunuz?

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

En fazla 5 dakika.

- 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



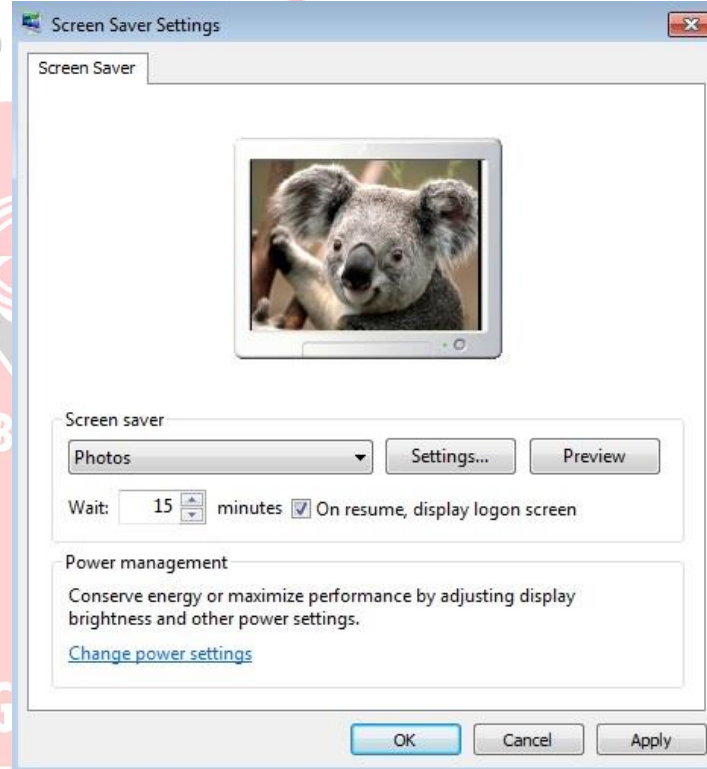
- Parolanın başkaları tarafından ***görülmemesi*** sağlanmalıdır.
- Sizden başka bir kimse kullanıcı hesabınızla işlem yapmamalıdır.
- Parolalarınızı korumazsanız başkalarının günahını da üstlenmek zorunda kalabilirsiniz

...

Ekran kilidi



Parola korumalı ekran koruyucusu



Press CTRL + ALT + DELETE to unlock this computer

Asım Genç Gökçe (SIRKET\aggokce) is logged on.

Parola Güvenliği



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

Bankalarası Kart Merkezi

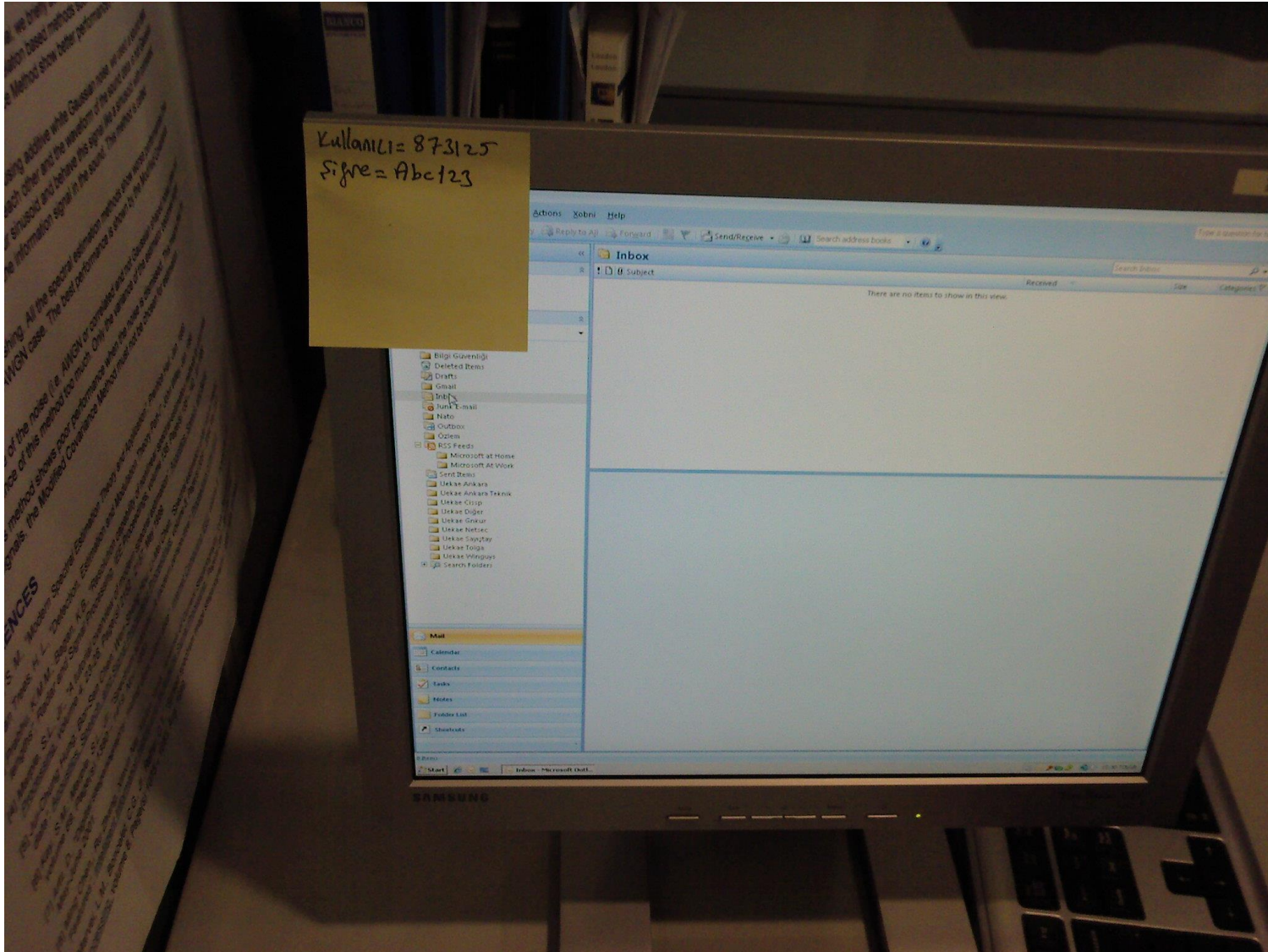


İlgi ve A

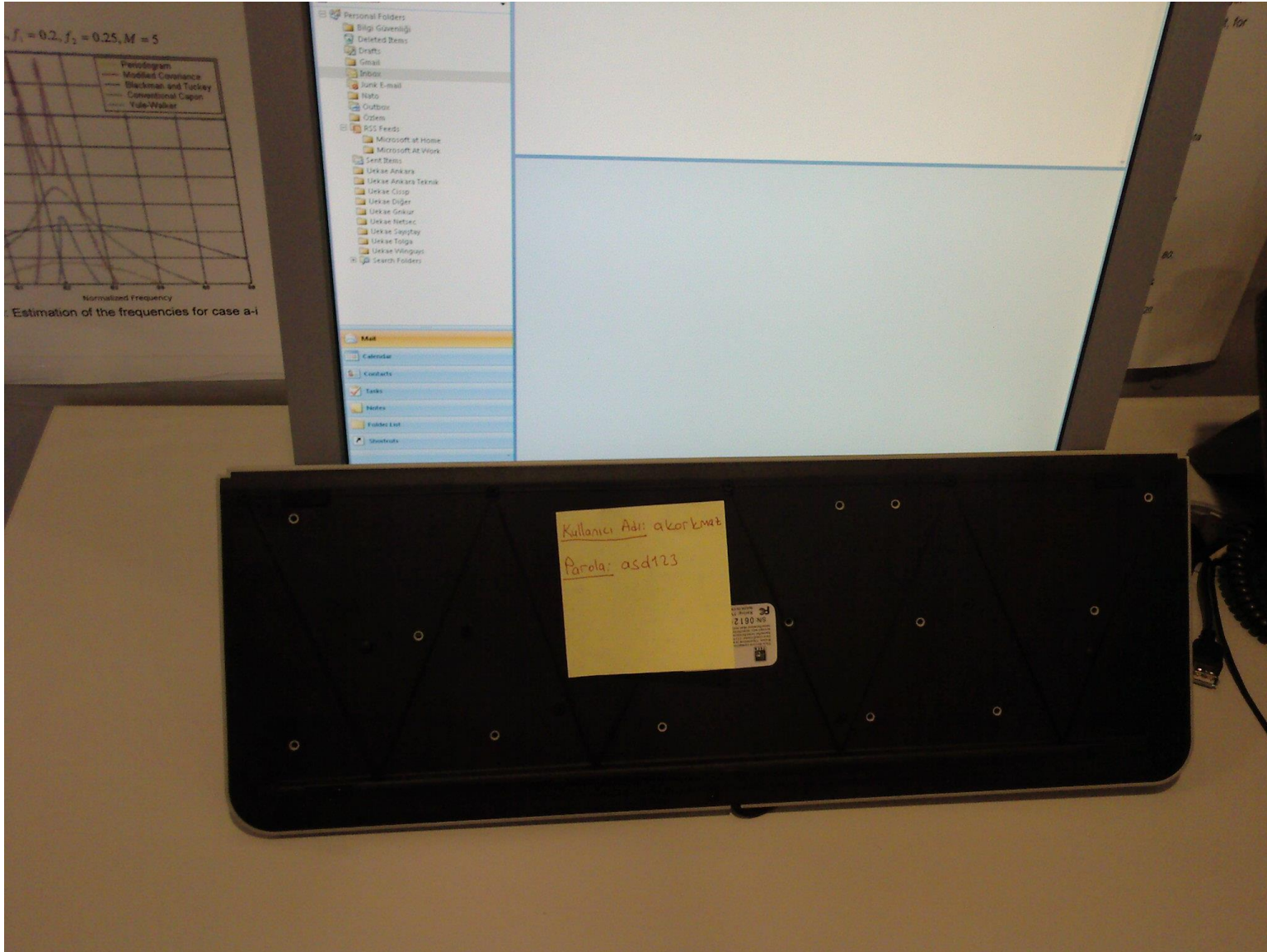
- En önemli kişisel bilgi, parolanızdır.
- Hiç kimseyle herhangi bir şekilde paylaşılmamalıdır.
- Mümkünse bir yere yazılmamalıdır. Yazılması gerekiyorsa güvenli bir yerde muhafaza edilmelidir.
- Güvenli olmadığını düşündüğünüz mekanlarda **kurumsal parolalarınızı** kullanmanızı gerektirecek uygulamaları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



Parolalar - Güvenli Muhafaza Edin



Parolalar - Güvenli Muhafaza Edin



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** (?, @, !, #, %, +, -, *, %)

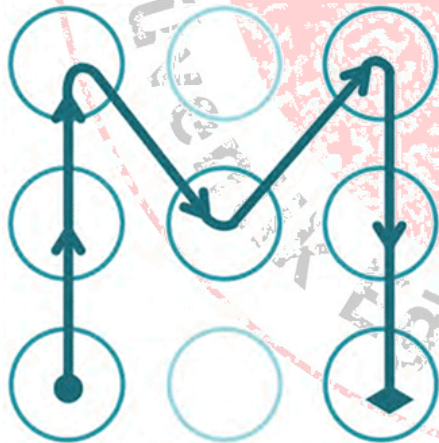
toplamda en az **8** karakter uzunluğunda.

Bilinen

MT1955@@zym123**

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

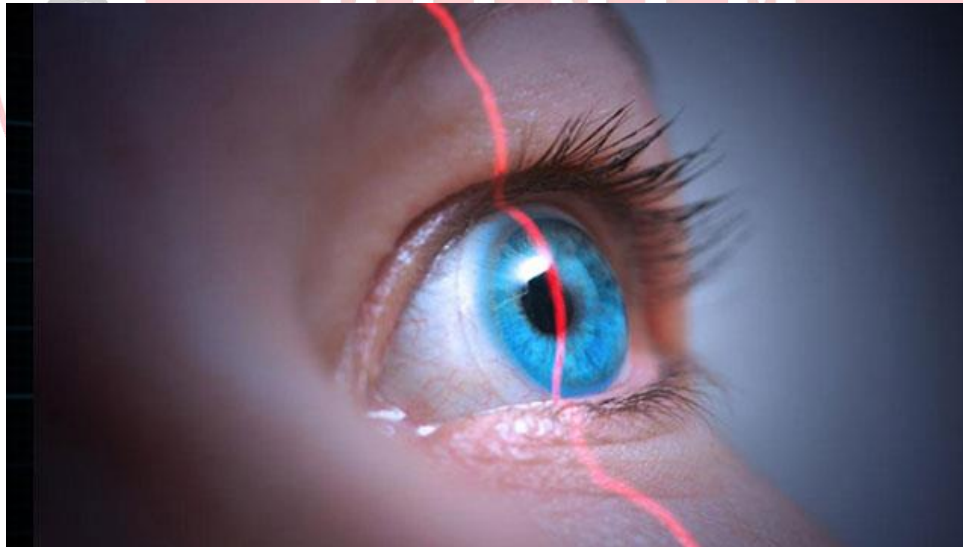
10 Yılda 15 milyon genç yarattık her yaştan. --> **10Y15mgyhy.**



Sahip Olunan



Bizim olan



Parolanızı Deneyin: Parola Ölçer

<http://www.bilgimikoruyorum.org.tr/?b223> yaparak ogrenelim



Bilgisayar ve Erişim Güvenliği: Parola Güvenliği

Yaparak Öğrenelim (Parola Ölçer)

Bilgisayar ve Erişim Güvenliği > Parola Güvenliği > Yaparak Öğrenelim (Parola Ölçer)

Parola denetleyicileri farklı düzeylerde kontroller yaparlar. Bazıları sadece temel prensipleri kontrol ederken bazıları çok daha farklı kriterleri hesaba katar.

Aşağıdaki parola alanına deneme amacı ile parolalar girerek puanlamalarını inceleyebilir ve kriterler hakkında bilgi alabilirsiniz. **Nasıl mı?**



Parolanızı Ölçün!

Parola: [Parolayı Göster](#) [Ekle](#)

Puan (%): 0% **Çok Zayıf**

Toplam puan: -100 (Fazla tekrar yokken toplam puan : -100)

Tipi Açıklama	Min. Sayı	Toplam sayı	Puan	Ceza	Toplam Puan
3 Kritik özellikler	3	0	10	-10	-10
3 Karakter sayısı *	5	0	10	-20	-20
3 Önerilen karakter sayısı	8	0	10	-10	-10
3 Küçük harf kullanımı *	1	0	10	-10	-10
3 Büyük harf kullanımı *	1	0	10	-10	-10
3 Rakam kullanımı *	1	0	10	-10	-10
3 Sembol kullanımı *	1	0	10	-10	-10
3 Rakamların aralarda kullanımı	1	0	10	-10	-10
3 Sembollerin aralarda kullanımı	1	0	10	-10	-10
2 Ardeşik harf kullanımı		0	0	-10	0
2 Ardeşik rakam kullanımı		0	0	-10	0
2 Klavye kalıpları kullanımı		0	0	-10	0
2 Tekrarlanan kısımlar var		0	0	-10	0

Bu parolalar ne kadar güçlü?

Aşağıdaki parolalar güçlü mü? Tıklayın öğrenin.

password Jane2008 t88t88 Foobar
Foobar99 qwertz Qw3rt2 71562563512
catecate catekate foo99foo99 12testtest
wolwOIWol Fooob Qtesse1Z

Parola Karşılaştırma Listesi

Parolalarınızı buraya ekleyerek karşılaştırın.

İşaret Kılavuzu

- Bu kriter karşılanmamaktadır. Parolanızı değiştirmelisiniz.
- Parolanız bu kriteri karşılamaktadır.
- Kriterin üzerine çıkmıştır. Bu kriter açısından parolanız son derece güçlü.
- Bu renkteki kriter yapılan son parola değişikliğinden etkilenebilir.
- 3 Bu kriter üç seviye içerir; ("Kaldı", "Gerekli", "Yeterli").
- 2 Bu kriter "Geçti" ve "Kaldı" şeklinde iki seviye içerir.

Sayfa Hakkında

Bu web sayfası herhangi bir sunucuya parola verisi aktarmamaktadır. Uygulama sadece sizin internet tarayıcınızda çalışmakta ve parola ölçümünüz gözlem ve tecrübelerine dayanmaktadır. Bu uygulama parolanızın güvenliğini garanti etmez. Amacımız sizin prensipleri öğrenmeniz ve daha uygun parolalar bulmanıza yardımcı olmaktır.

Bu uygulamanın orijinal kaynak kodu CC-GPL-2.0 lisansı altında, orijinal ve değiştirilmiş olarak dağıtılabilir.

• Çeşitli parolalar deneyerek karmaşık parola tasarlayın.

• (Gerçek parolanızı girmeyin!)

- Kişisel bilgilerle ilişkili mi? (çocuđunuzun 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 paroladır. 8 karakterden az.

antalya

Özel isim. Kullanıcının doğum yeri ise zayıf bir paroladır.

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

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	qqqqqq	qqqq
55555	44444	33333	22222 aaa	sql	file
5555	4444	3333	2222 home	work	intranet
555	444	333	222 private	market	coffee
55	44	33	22 student	account	academia
5	4	3	2 unknown	anything	letitbe
11111111	00000000	0987654321	money	campus	explorer
1111111	0000000	987654321	nobody	codeword	codename
111111	00000	87654321	secure	public	system
11111	0000	7654321	superuser	share	super
1111	000	654321	owner	backup	database
111	00	54321	manager	temporary	ihavenopass
11		4321	Internet	internet	example
1		321	work123	home123	mypcl123
		21	abc123	pwl123	root123
		12	admin123	admin12	admin1
			default	foobar	foofoo
			test	rootroot	root
			pass	Login	login
			zxcvbn	zxcvb	zxcxz
			qlw2e3	qweasdzxc	asdfgh
			qweasd	qwerty	qweewq
			Admin	admin	alb2c3
			123asd	123qwe	123abc

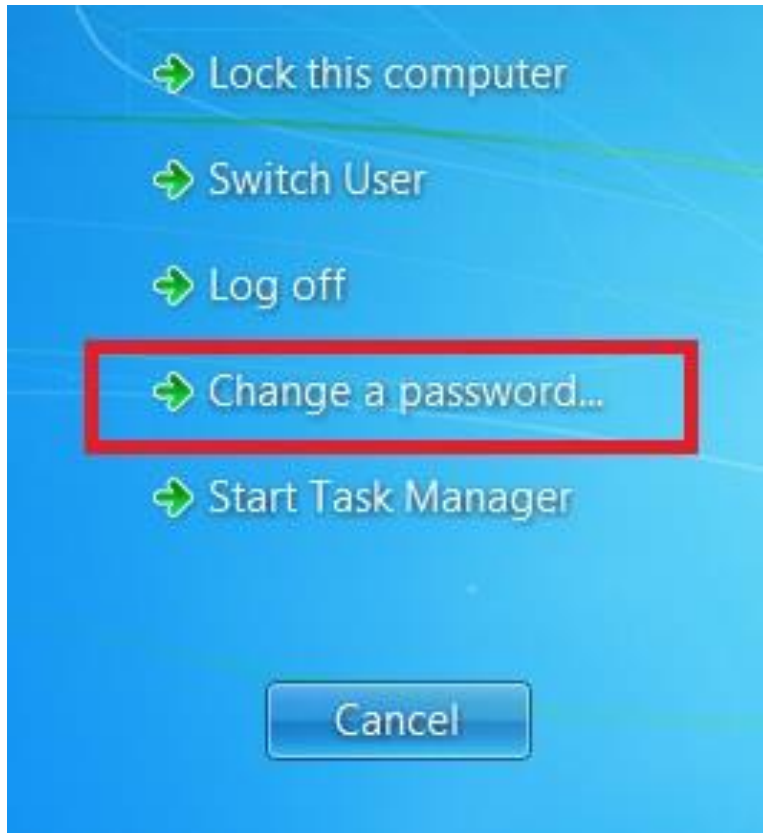


aaaaa	aaaa
foo	job
killer	games
forever	freedom
windows	monitor
domain	access
customer	cluster
desktop	security
office	supervisor
server	computer
oracle	business
nopassword	nopass
lovel23	boss123
test123	qwel23
pass123	pass12
password123	password12
temptemp	testtest
adminadmin	mypassword
Password	password
zxcxz	qazwsxedc
asdzxc	asdds
qwewq	nimda
1q2w3e	1234qwer
123321	12321

Conficker

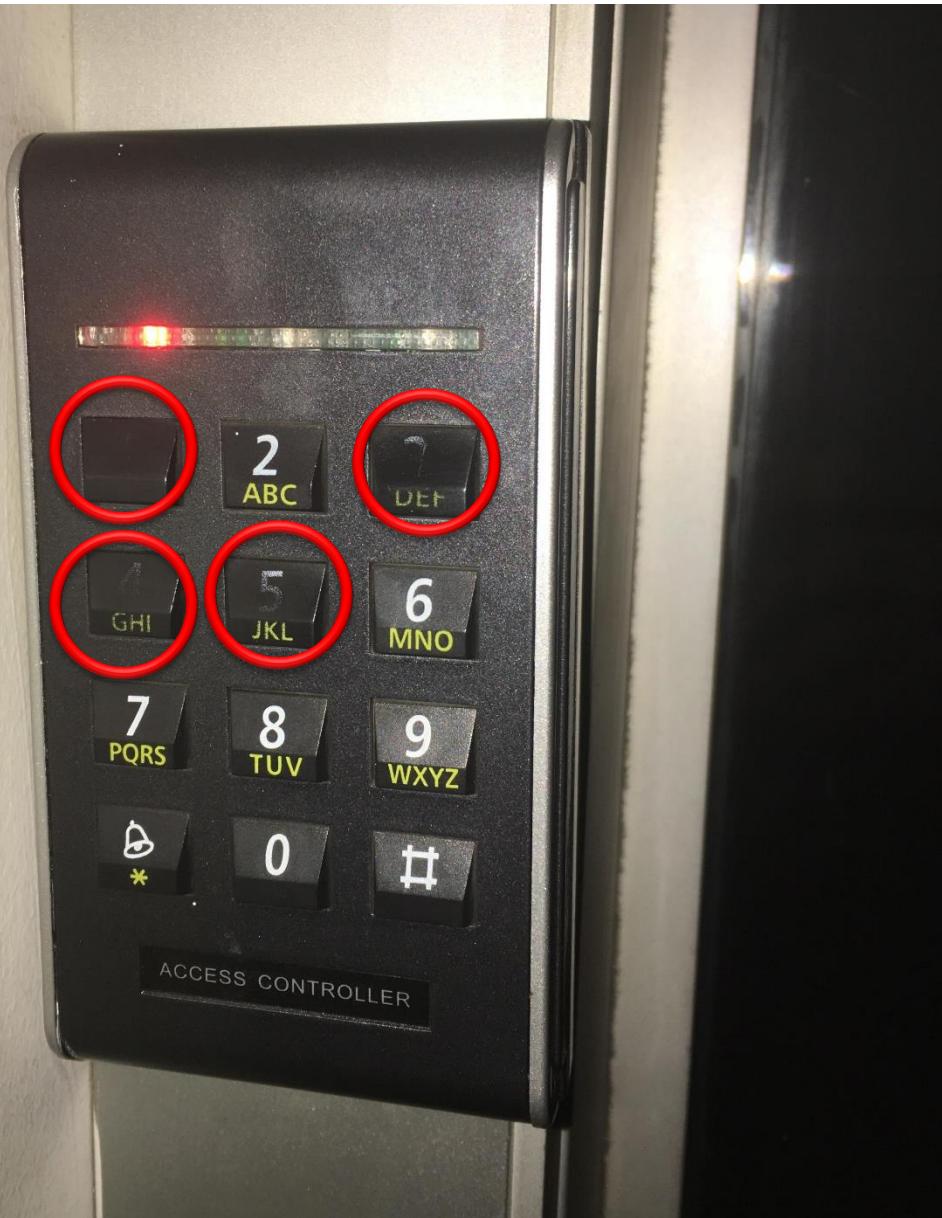
*solucanının denediği
parola örnekleri!*

Parola Güvenliği – Düzenli olarak değiştirilmeli



Parola Güvenliđi – Düzenli olarak deđiřtirilmeli





**Bilin bakalım
parola nedir?**

Tabii ki

1453

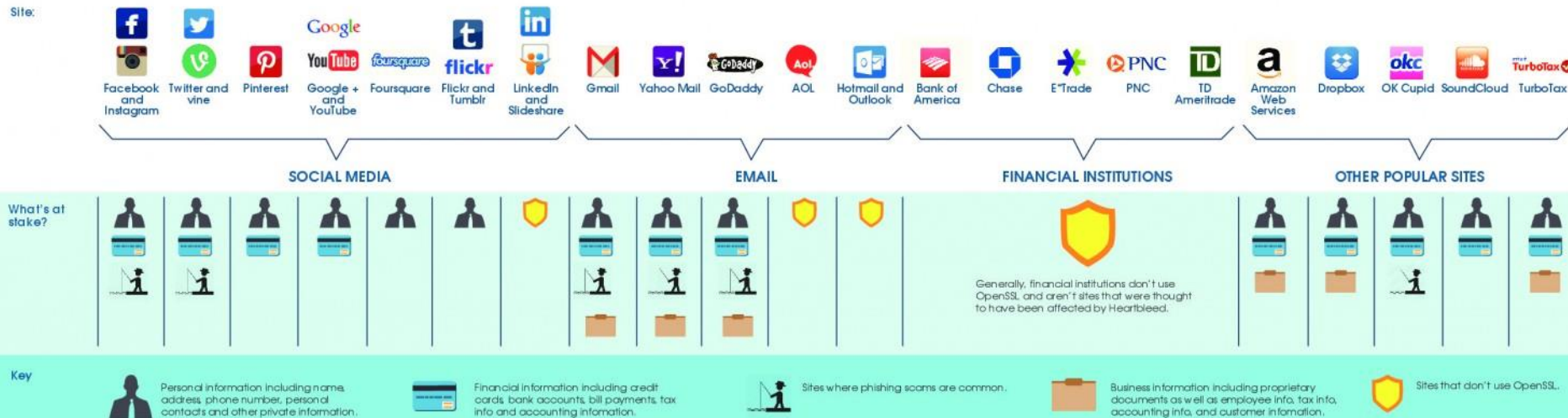
Parolalar **sakız** gibidir ...



Başkalarıyla **paylaşılmaz**,
ara sıra **yenilemek** gerekir,
ortalıkta bırakılmaz.

A large red heart with red liquid dripping down from its base, set against a background of binary code and a grid of smaller hearts.

THE PASSWORDS YOU SHOULD CHANGE AND THE PEOPLE YOU SHOULD TRUST





Hesabını Güvende Tutmak

Twitter hesabın için şifre belirlediğinde, şirketteki kimsenin görmemesi için bir maskeleyme 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

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

Eğer Shakespeare
eserlerini bilgisayarda
yazsaydı



Upgrade yapmak veya yapmamak, işte bütün mesele bu!

Güvenli olmayan yazılımlar nelerdir?



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



Eğitim ve Araştırma



"Open Source Security Bug Bounty"

Dosya Erişim ve Paylaşım Güvenliği

SİBER GÜVENLİK
ENSTİTÜSÜ

- Oluřturulan dosyaya erişecek kişiler ve hakları “**bilmesi gereken**” prensibine göre belirlenmelidir.
- Erişecek kişilerin hakları yazma, okuma, deđiřtirme ve alıřtırma yetkileri göz önüne alınarak oluřturulmalıdır.
- Verilen haklar belirli zamanlarda kontrol edilmeli, deđiřiklik gerekiyorsa yapılmalıdır.
- Eđer paylaşımlar aılıyorsa ilgili dizine sadece gerekli haklar verilmelidir.



Paylaştırılmış klasörlerden gelebilecek tehlikeler nelerdir?

- Sizin haberiniz olmadan aynı ağıdaki bir kiři paylaştığınız dosyalara **erişebilir, deđiřtirebilir hatta silebilir,**
- paylaşımlar çođu zaman **virüslerin ve zararlı yazılımların** yayılmak için kullandıkları alanlardır,
- bir dosyanın telif haklarını ***isteyerek veya istemeyerek*** ihlal etmiş olabilir ve yasaları çiđnemiş olabilirsiniz.





- Çalınmalara karşı fiziksel güvenlik sağlanmalıdır.
- BIOS ayarlarını başkasının değiştirmesini engellemek için BIOS giriş 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.)





- 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.

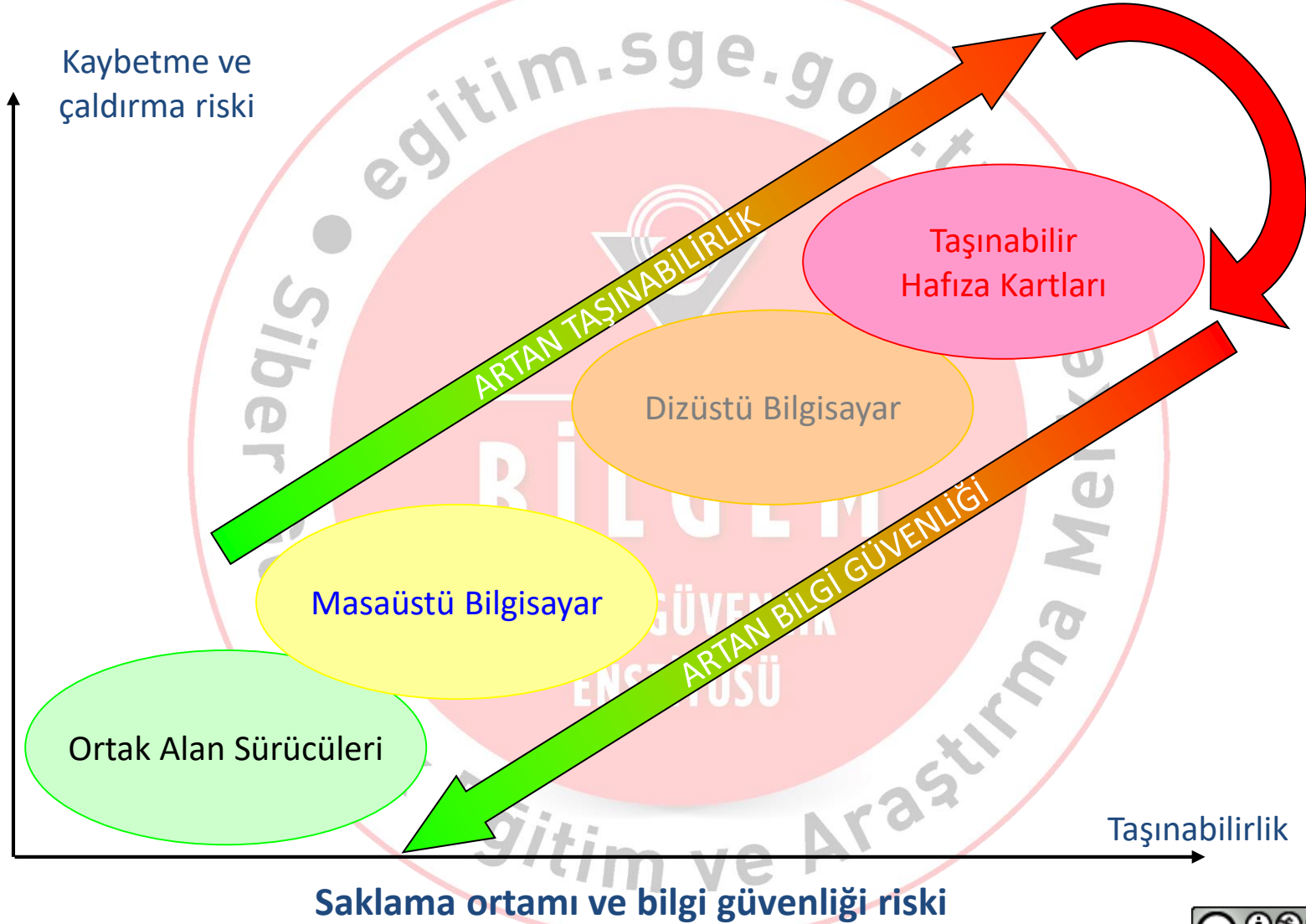
Bir USB bellek, 1 milyon adet kağıtta yer alan bilgi kadar veri içerebilir.

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



Let's Go Digital

Saklama Ortamlarının Doğru Kullanımı



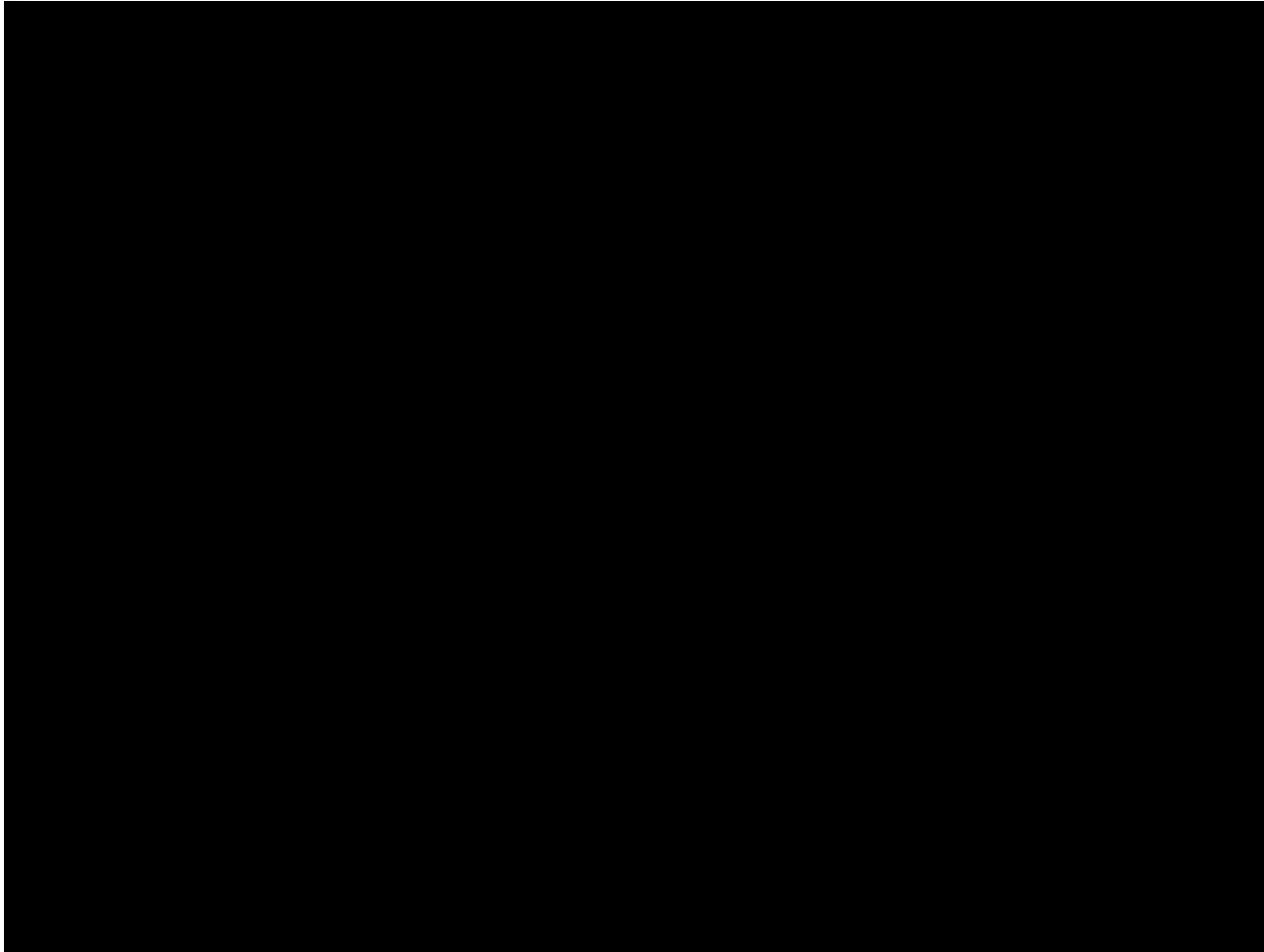
Zararlı Yazılımlar



- 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%



What have we learned from history?

- 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

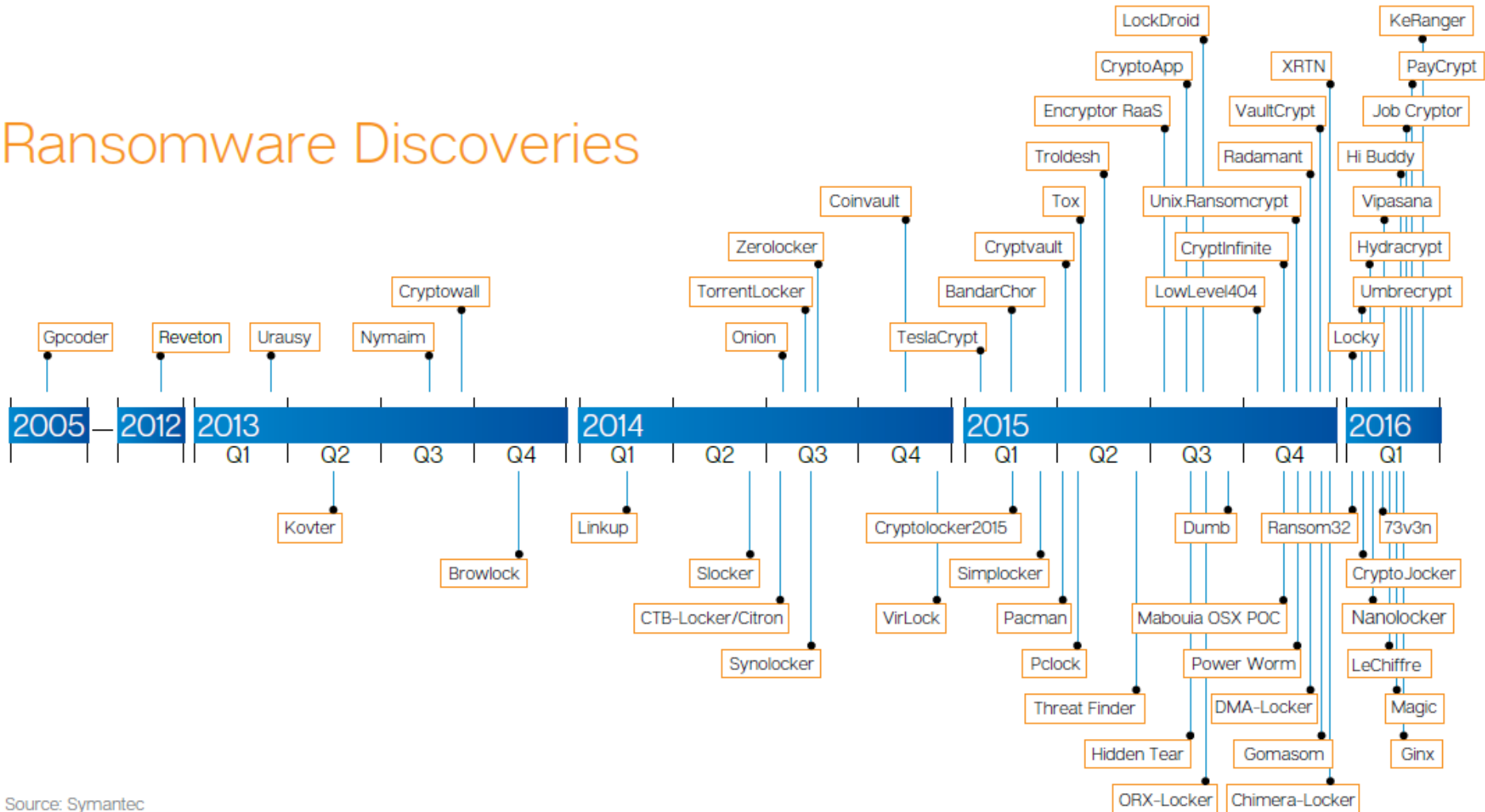
- E-posta eklerini çalıştırarak
- Güvensiz sitelerden indirilen dosyalar ile
- Paylaşım ortamlarındaki dosyalar aracılığı ile



- 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

Ransomware Discoveries



Source: Symantec

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

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: Normalde insanların tanımadıkları biri için yapmayacakları şeyleri yapmalarını sağlama sanatıdır.
- Teknoloji kullanımından çok insanların hile ile kandırılarak bilgi elde edilmesidir.





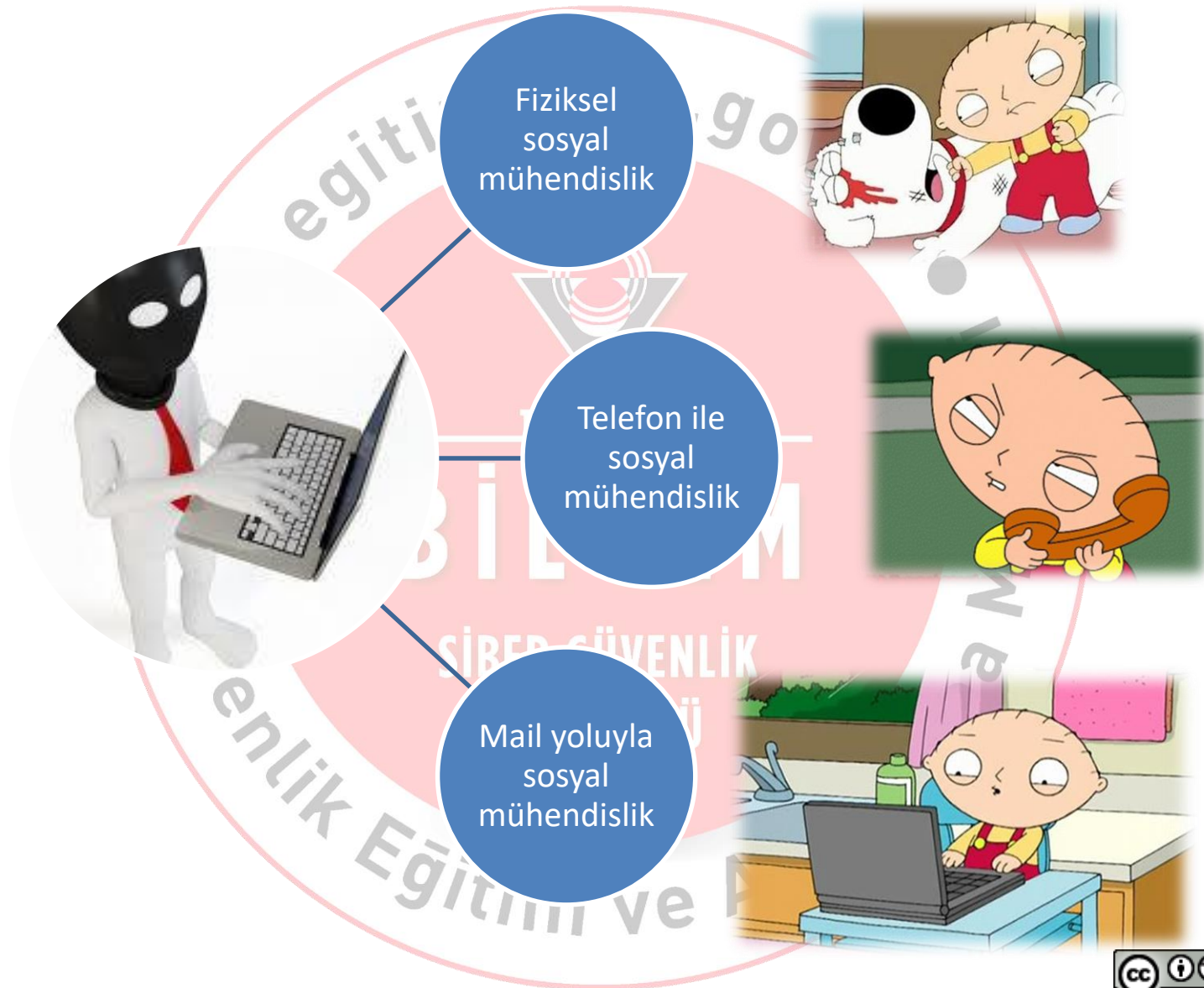
- Çoğu zaman basit dolandırıcılığa çok benzese bile, bu terim genelde bilgi sızdırmak veya bir bilgisayar sistemine sızmak üzere yapılan numaralar için kullanılır.
- Bu durumların büyük çoğunluğunda saldırgan, kurban ile yüz yüze gelmez.
- Kullandığı en büyük silahı, insan zaafiyetleridir.

İçinde insan olan
her süreç bir şekilde
istismar edilebilir!!



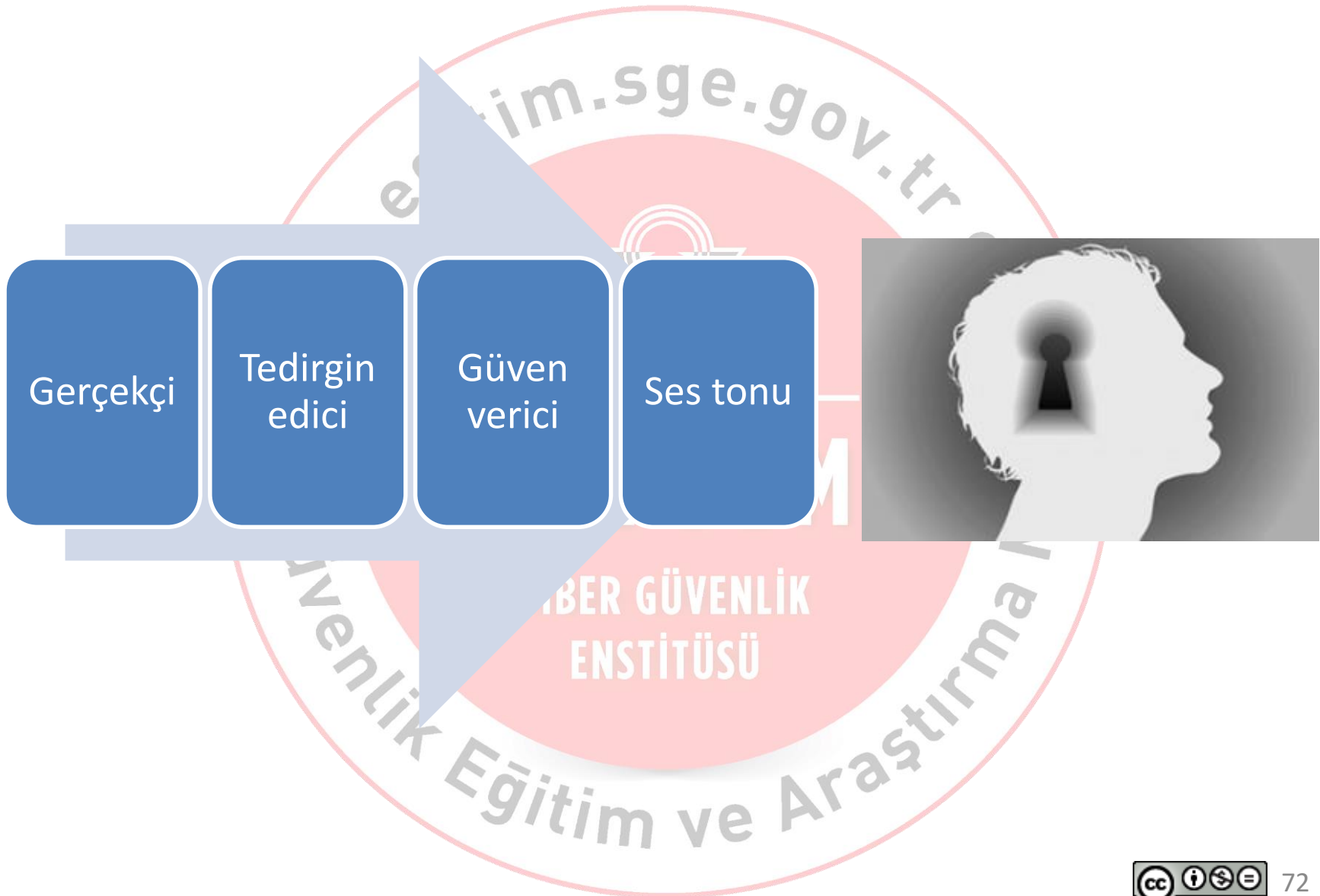






«Teknolojiyi kullanarak (*internet, cep telefonu,..*)
başkasına zarar vermek için tasarlanmış,
kasıtlı ve tekrarlanan *düşmanca davranış*.»

SİBER GÜVENLİK
ENSTİTÜSÜ



Gerçek Örneklerle Sosyal Mühendislik

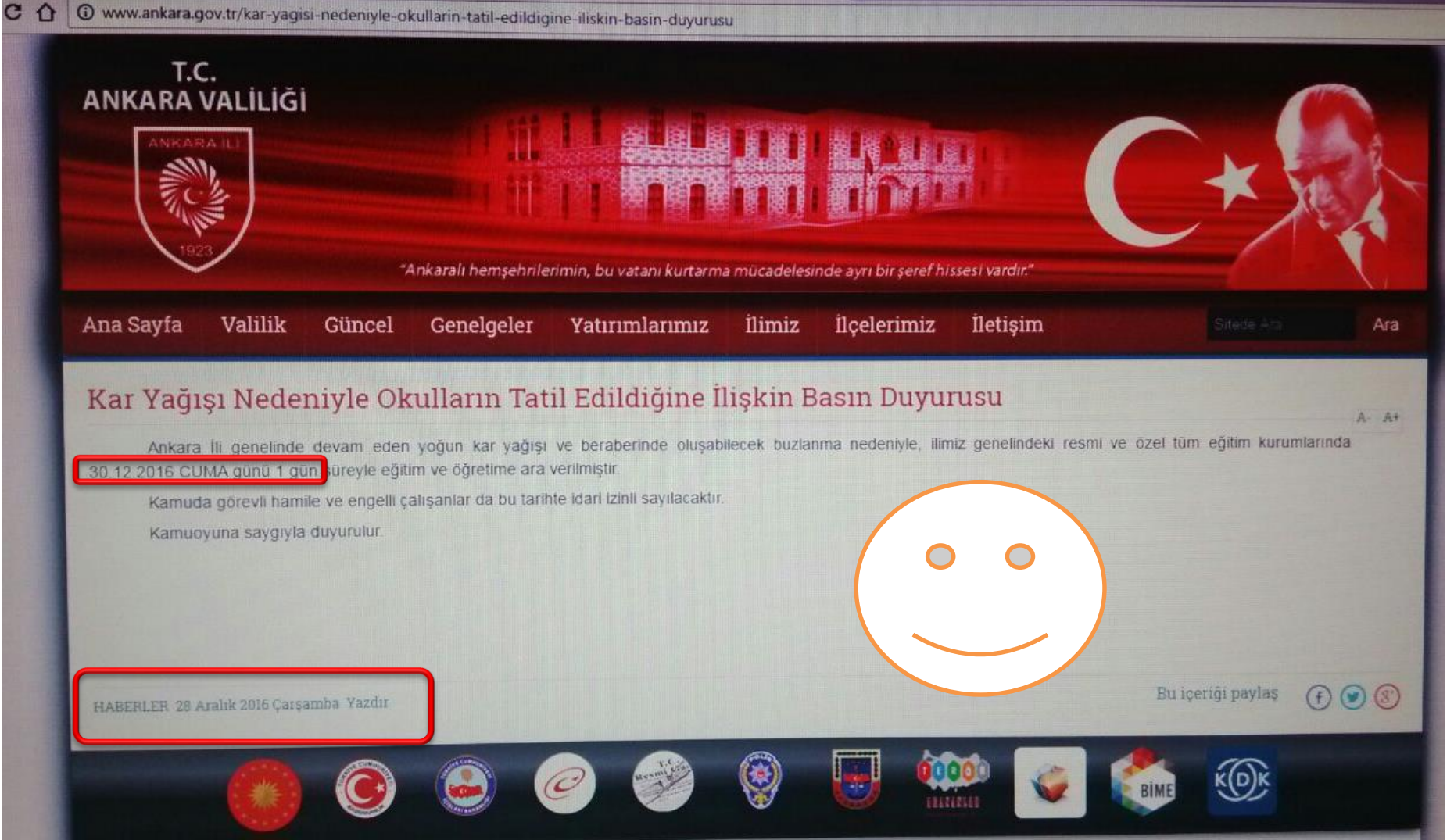
SİBER GÜVENLİK
ENSTİTÜSÜ



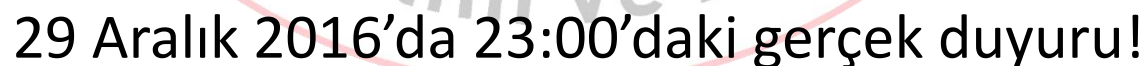
https://www.youtube.com/watch?v=Kz_soitDto

Bankalarası Kart Merkezi

29-30 Aralık 2016 Ankara'da Kar Tatili Hikayesi

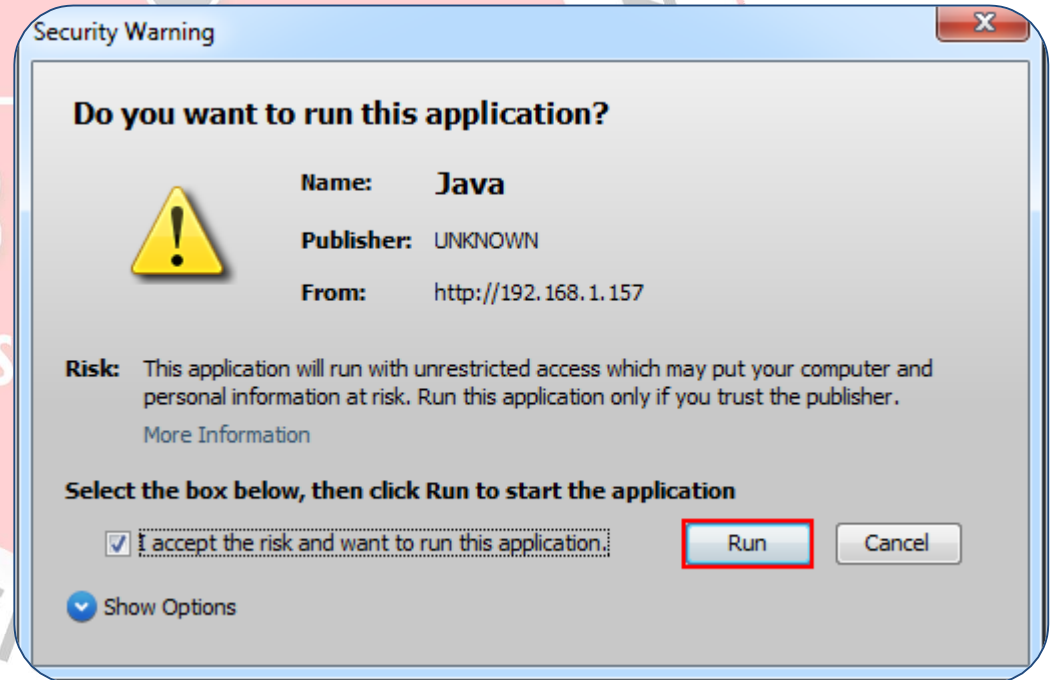


29 Aralık 2016 saat 20:00'dan önce sosyal medyada yayılan bir resim!



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. »





- 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.

TÜBİTAK
SİBER GÜVENLİK
ENSTİTÜSÜ

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

MSN Hotmail - Message - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites RSS Print Mail News Groups

Address http://by20fd.bay20.hotmail.msn.com/cgi-bin/getmsg?curmbox=F0000000058a=d1b07156b64997ab23b1e520b1cd5224&msg=MSG1108348558.8&ShowImages=1
bariserdogan@hotmail.com

Free Newsletters | MSN Featured Offers


Reply Reply All Forward Delete Junk This is not Junk Put in Folder Print View Save Address

From: Garanti24 <guncelleme@garanti.com.tr>
Reply-To: <guncelleme@garanti.com.tr>
Sent: Monday, February 14, 2005 2:35 AM
Subject: Garanti Bankası Guncelleme Formu (Lutfen Okuyun)

MIME-Version: 1.0
Received: from sam.secure-dns.net ([67.18.210.226]) by mc6-f40.hotmail.com with Microsoft SMTPSVC(6.0.3790.211); Sun, 13 Feb 2005 18:35:58 -0800
Received: from dsl81-215-29416.adsl.ttnet.net.tr ([81.215.114.232] helo=User) by sam.secure-dns.net with esmta (Exim 4.43) id 1D0W5K-0000Sk-Q; Sun, 13 Feb 2005 19:35:39 -0700
X-Message-Info: uX4bQusXWIK7S83jbratCc69a2NopDsa7bx79Fjh0=
X-MSMail-Priority: High
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
X-Antivirus-Scanner: Clean mail though you should still use an Antivirus
X-AntiAbuse: This header was added to track abuse, please include it with any abuse report
X-AntiAbuse: Primary Hostname - sam.secure-dns.net
X-AntiAbuse: Original Domain - hotmail.com
X-AntiAbuse: Originator/Caller UID/GID - [0 0] / [47 12]
X-AntiAbuse: Sender Address Domain - garanti.com.tr
X-Source:
X-Source-Args:
X-Source-Dir:
Return-Path: guncelleme@garanti.com.tr
X-OriginalArrivalTime: 14 Feb 2005 02:35:58.0326 (UTC) FILETIME=[EA4EB960:01C5123D]

We've identified this mail as junk. Please tell us if we were right or wrong by clicking Junk or Not Junk

Junk Mail Not Junk Mail

 **GarantiBank**

Sayın Musterimiz...

Bankamızın siz müşterilerinin işlemlerini daha da hızlandırması için yılda bir kez bilgi guncellemesi yapacaktır. Hesabınızla ilgili işlemleri ve size daha iyi bir hizmet sunabilmemiz için aşağıda belirtilen Bilgi guncelleme sayfası üzerinden veya T.C Garanti Bankası subemizden bilgilerinizi teyit etmeniz gerekmektedir. Müsteri No, Parola ve 2. Güvenlik Sifrenizi bilmiyorsanız boş bırakabilirsiniz. Bos bıraktığınız takdirde bankamız yetkilileri size verdiğiniz telefon numarası ile ulaşarak bilgi teyidi alacaklardır...

<https://www.onlinebankacilik.net/form/>

Eğer yukarıdaki link çalışmıyorsa lütfen aşağıdaki linki kullanınız:


<https://http://216.193.252.20/form/>

DIKKAT: Lütfen Garanti Bankası üzerinden gelmeyen mailleri dikkate almayınız. Bu guncelleme sadece www.onlinebankacilik.net ve www.garanti.com.tr adreslerinden yapılmaktadır.

TESEKKURLER.....

Oktay SERHAT
GARANTI BANKASI A.Ş.

Done Internet



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

Garanti 24 Bilgi Güncelleme Formu - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites

Address http://www.onlinebankacilik.net/form/ Go Links

GarantiBank

Türkiye genelinde toplam 915 noktadaki Garanti 24'lerden, para alıp vermekten çok daha fazlasını yapabilirsiniz. Garanti24'leri kullanarak zaman kazanırsınız.Paracard, Bonus Card, Shop&Miles veya Garanti Card ile günün 24 saati, tatil günlerinde, mesai saatleri dışında; ihtiyacınız olduğu anda birçok işlemi Garanti 24'leri kullanarak yapabilirsiniz. Bankamızın siz müşterilerinin işlemlerini dahada hızlandırması için yılda bir bilgi güncellemesi yapacaktır.Lütfen aşağıdaki formu doldurunuz.Müşteri No,Parola ve 2. Güvenlik Şifrenizi bilmiyorsanız bos bırakabilirsiniz.Bos bıraktığınız takdirde bankamız yetkilileri size verdiğiniz telefon numarası ile ulaşarak bilgi teyidi alacaklardır...

Aşağıdaki bütün alanları lütfen eksiksiz olarak doldurunuz.

KREDİ KARTI BİLGİLERİNİZ:

Ad Soyad:

Kart No: Kredi kartınızın ön yüzündeki 16 haneli rakam.

Cvv2 Kodunuz: Kartınızın arka yüzündeki son 3 rakam.

Son Kullanma Tarihi: Kartınızın ön yüzünde gösterildiği şekilde giriniz.

ATM Pin: Atm Pininizi doğru olarak giriniz.

HESAP BİLGİLERİNİZ:

Müşteri No:

Parola:

2. Güvenlik Şifrenizi: (İnternet bankacılığı için kullanmakta olduğunuz 2. şifreniz.)

GÜVENLİK BİLGİLERİNİZ:

ANNENİZİN KIZLIK SOYADI:

İLETİŞİM BİLGİLERİNİZ:

ADRESİNİZ:

ŞEHİR:

İLÇE:

TELEFON:

CEP TELEFONU:

E-POSTA ADRESİNİZ:

Tamam

Kart şifrenizi bilmiyor veya hatırlamıyorsanız şifrenizi belirlemek için 444 0 333 Alo Garanti'yi arayabilirsiniz.

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\$)

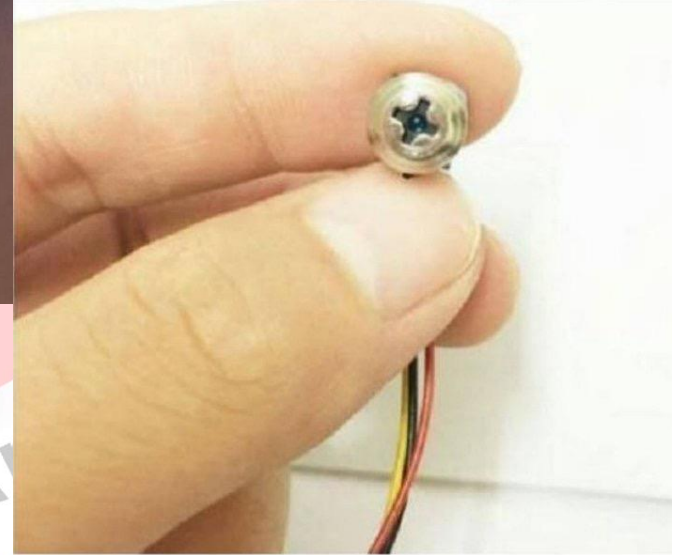
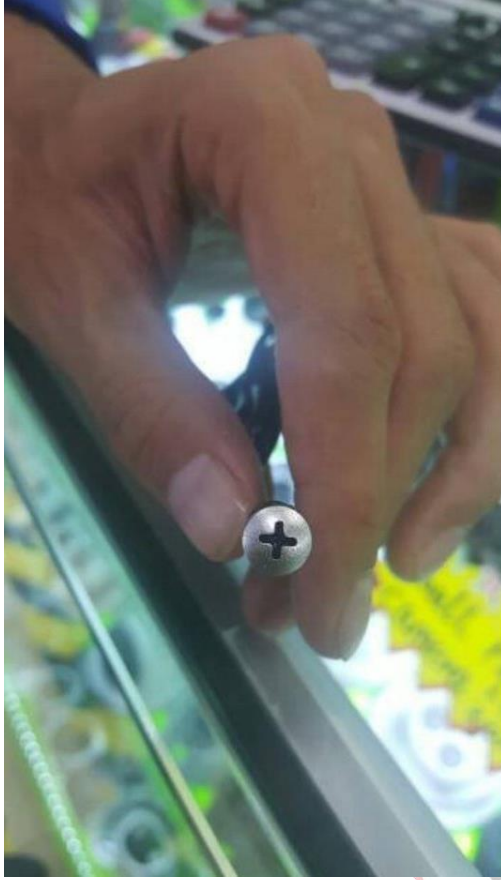


Kameralı gözlük
(79.99\$)

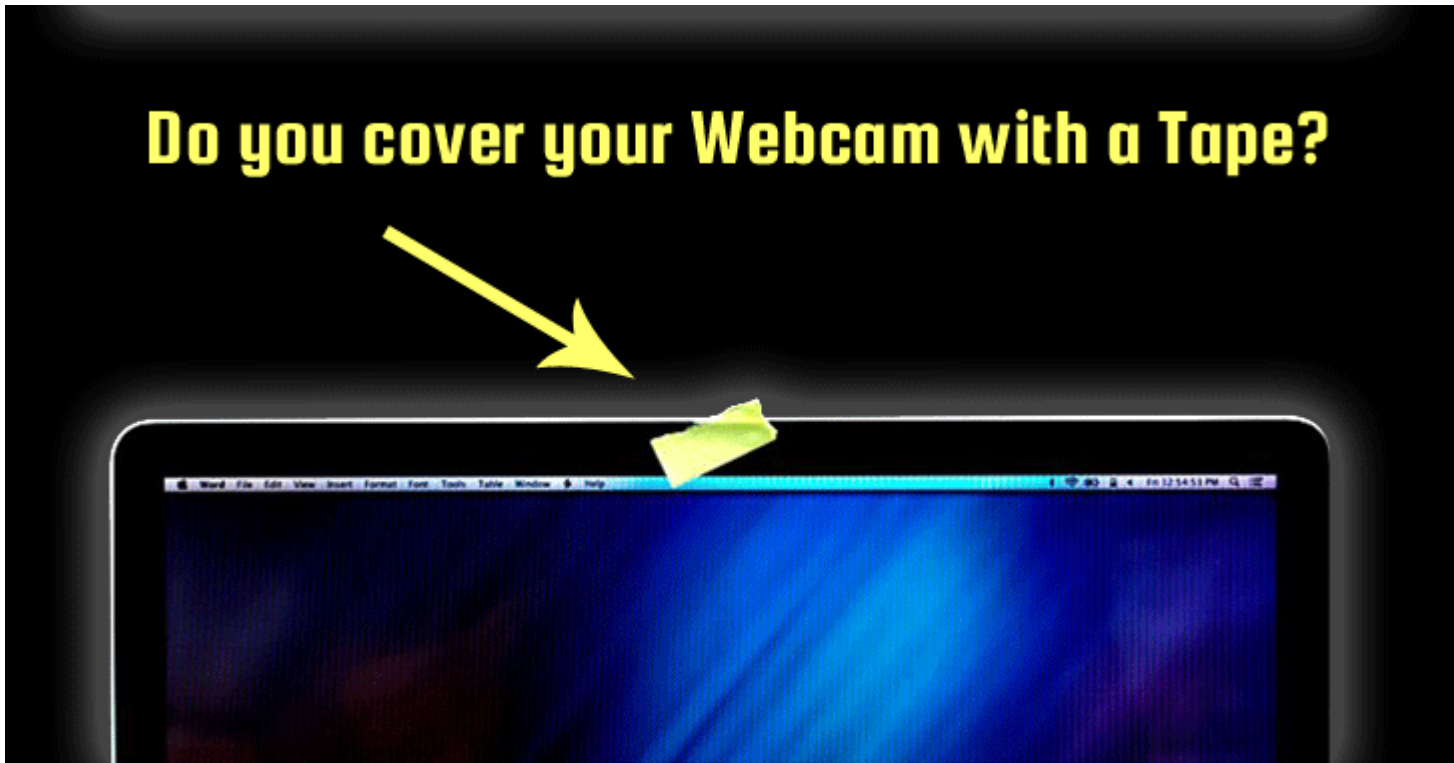
Tarafımızca başka kurumlara yapılan sosyal mühendislik saldırılarından bazı örnekler

1. kayıt:  2. kayıt:  3. kayıt: 





Do you cover your Webcam with a Tape?



- Facebook CEO [Mark Zuckerberg](#)
- FBI Director [James Comey](#)
- Security Consultant [Kevin Mitnick](#)
-



- 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.

- 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.

Web ve E-posta Güvenliği

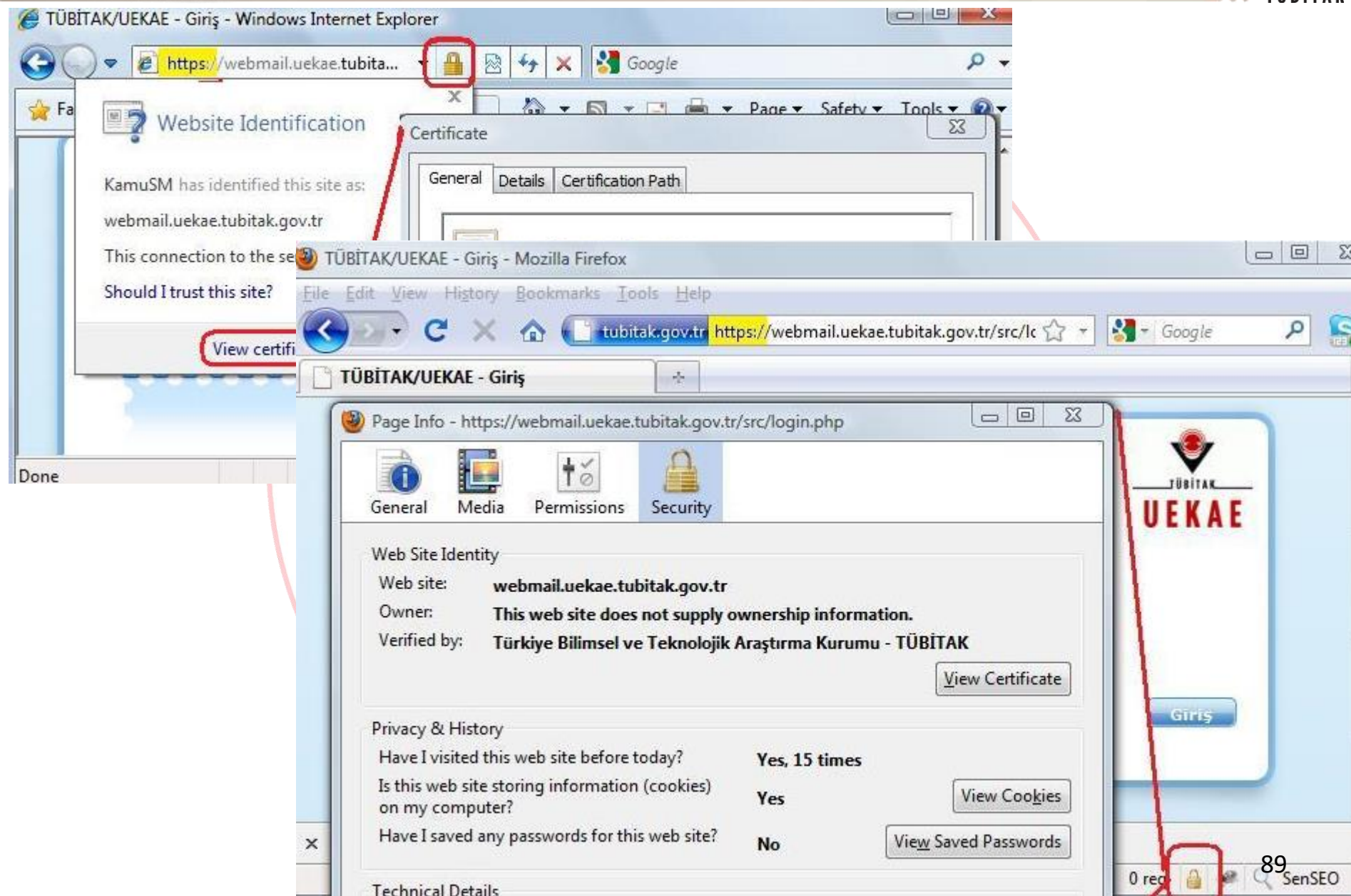
SİBER GÜVENLİK
ENSTİTÜSÜ

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

Peki bu protokoller ile sađlanan veri alışverişı ne kadar güvenli



Web Güvenliği



The screenshot displays a Windows Internet Explorer browser window with the address bar showing <https://webmail.uekae.tubitak.gov.tr>. A red box highlights the lock icon in the address bar. A "Website Identification" dialog box is open, showing the site's identity and a warning: "Should I trust this site?". A red box highlights the "View certificate" link. A "Certificate" dialog box is also open, showing the "General" tab. In the background, a Mozilla Firefox browser window is visible, showing the same URL and a "Page Info" dialog box. The "Page Info" dialog box has the "Security" tab selected, showing the "Web Site Identity" section with the following information:

Web Site Identity	
Web site:	webmail.uekae.tubitak.gov.tr
Owner:	This web site does not supply ownership information.
Verified by:	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK

Below the "Web Site Identity" section, the "Privacy & History" section is visible, showing the following information:

Privacy & History	
Have I visited this web site before today?	Yes, 15 times
Is this web site storing information (cookies) on my computer?	Yes
Have I saved any passwords for this web site?	No

At the bottom of the "Page Info" dialog box, the "Technical Details" section is partially visible. The background Firefox window also shows a "Giriş" (Login) button and a "SenSEO" logo in the bottom right corner.

HTTP/FTP Eriřimlerinde Nelere Dikkat Etmeli?

- řifrenizin deđiřmesi gerektiđini belirten web sayfaları ya da e-posta mesajlarına,
- çok fazla bilinmeyen,
- bahis siteleri,
- pornografik ierik 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%

- *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.

From : "Marvene Zelda" <tamasinellsihphgdm@star.optdeals.com>
To : "Tamas" <leprechaun111@hotmail.com>
Subject : Get Cash Out Now! Our New Short Form Gets You..... ayscaffygs
Date : Thu, 26 Sep 2002 03:11:55 -0700
Reply Reply All Forward Put in Folder... Printer Friendly Version



MORTGAGE RATE ABOVE 4.50%?

WE WILL BEAT
Any Mortgage RATE
For The Next 5 DAYS

The shortest form on the Internet- under ONE minute
click here

 © 2002 Mortgage Corporation-Equal Housing Opportunity

INFORMATION FOR iREWARDSTECH RECIPIENTS:
To subscribe or unsubscribe from the iREWARDSTECH mailing list, [click here.](#)



- 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.
- Bilmediđiniz haber ve e-posta gruplarına üye olmamamız.

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



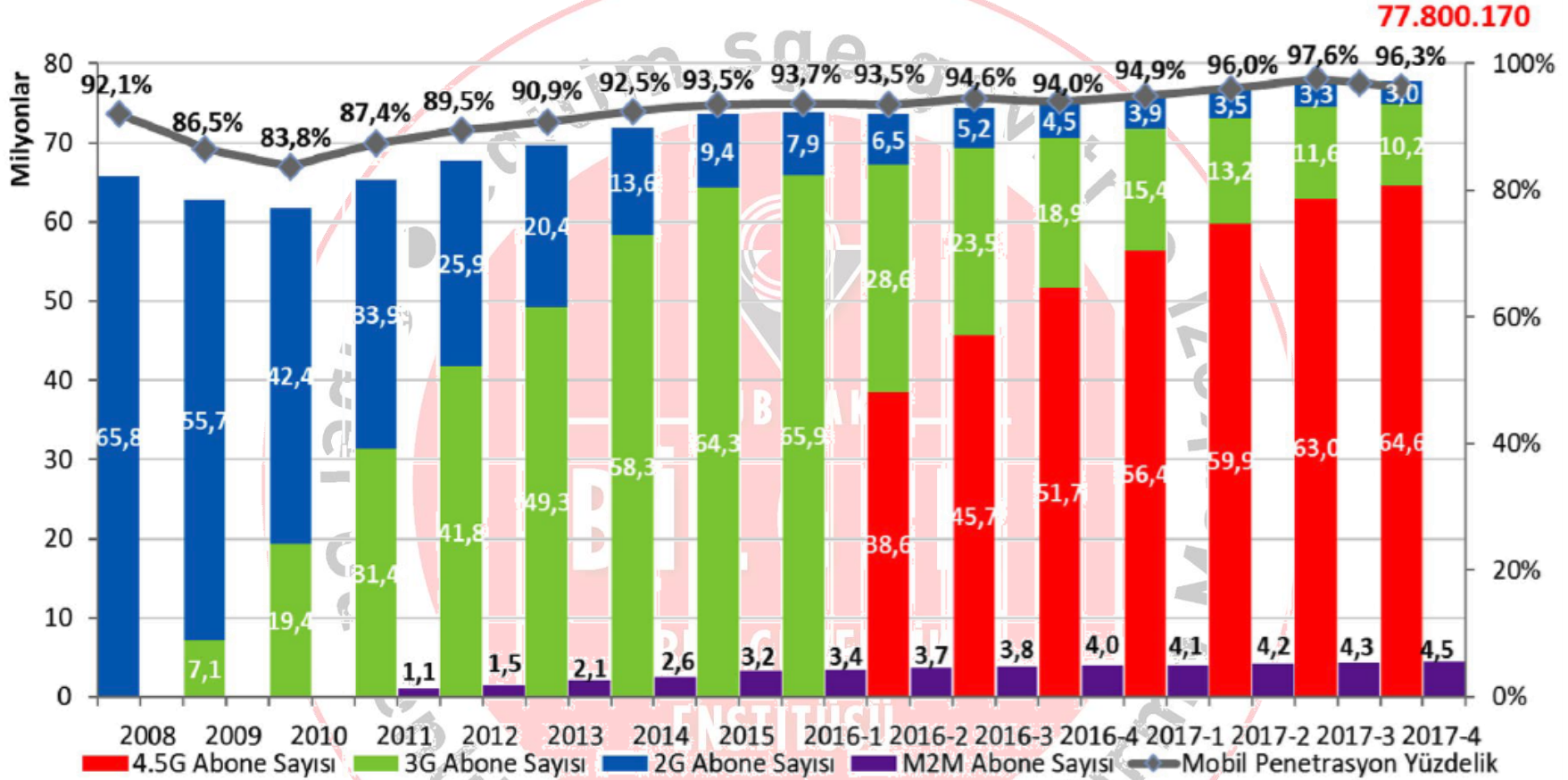
Mobil Cihaz Güvenliği

SİBER GÜVENLİK
ENSTİTÜSÜ

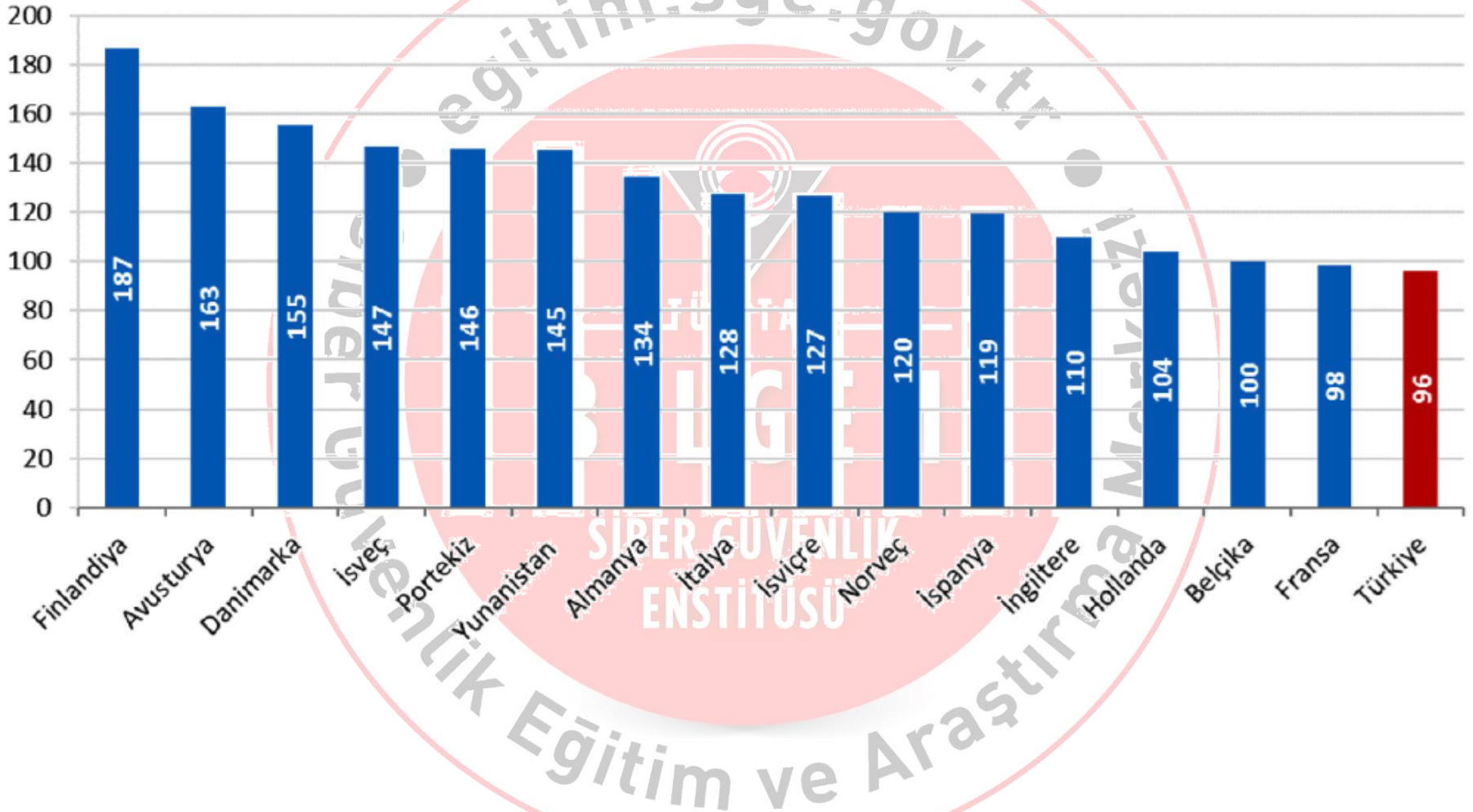


- 2000 yılında dünyada muhafaza edilen bilginin sadece dörtte biri dijitalken: **%25**
- 2013'te dijital olmayan verilerin oranı yüzde 2: **%98**
- 2016 yılında **5** bağlantıdan **4**'ü mobil platformlardan

Türkiye'deki Toplam Mobil Abone Sayısı ve Nüfusa Göre Penetrasyon



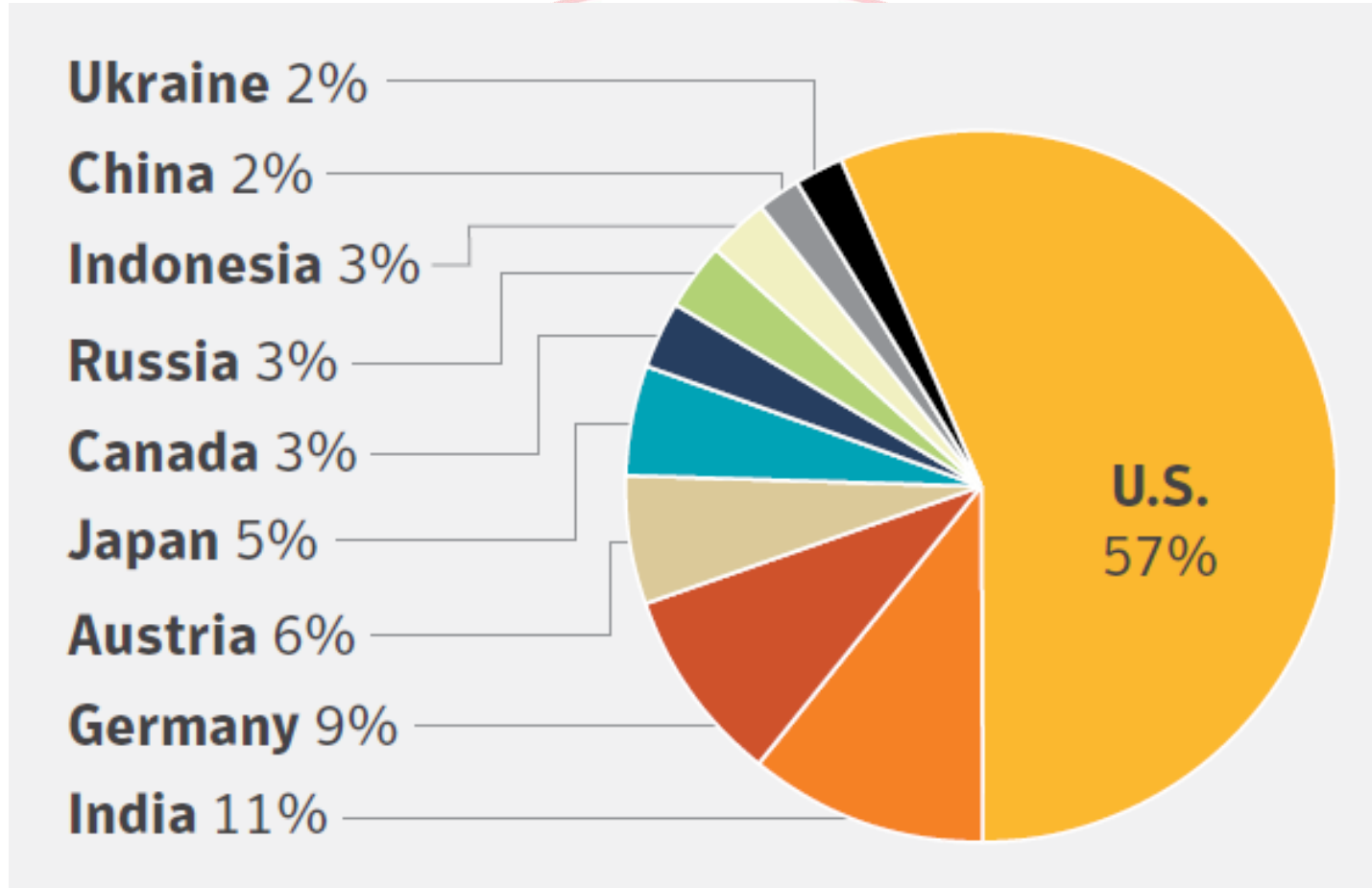
Türkiye ve Bazı Avrupa Ülkelerinin Mobil Penetrasyon Oranları, %



BTK Pazar Verileri Raporu, 2017-4.

<https://www.btk.gov.tr/uploads/pages/2017-q4.pdf>

Mobil Zararlı Yazılımların Ülkelere Göre Dağılımı



IS YOUR SMARTPHONE **SPYING** ON YOU?

PRIVACY & SECURITY SETTINGS ALL **IPHONE** USERS SHOULD KNOW ABOUT

5 tips Carnegie Mellon's CyLab &
Professor Norman Sadeh,
in Carnegie Mellon University's
School of Computer Science

Carnegie Mellon University
CyLab
Security and Privacy Institute

1

“Frequent Locations” setting

Settings > Privacy > Location Services > System Services > Frequent Locations
Turn this setting off if you don't want Apple to track the locations you frequently visit (home, work, favorite lunch spot, etc.)

2

“Erase Data” setting

Settings > Touch ID & Passcode > Erase Data
Set this to green if you want all of the data on your iPhone to erase after 10 failed passcode attempts.

3

“Advertising Identifier” setting

Settings > Privacy > Advertising
Regularly reset your “advertising identifier” if you don't want ad companies to build extensive profiles about you.

4

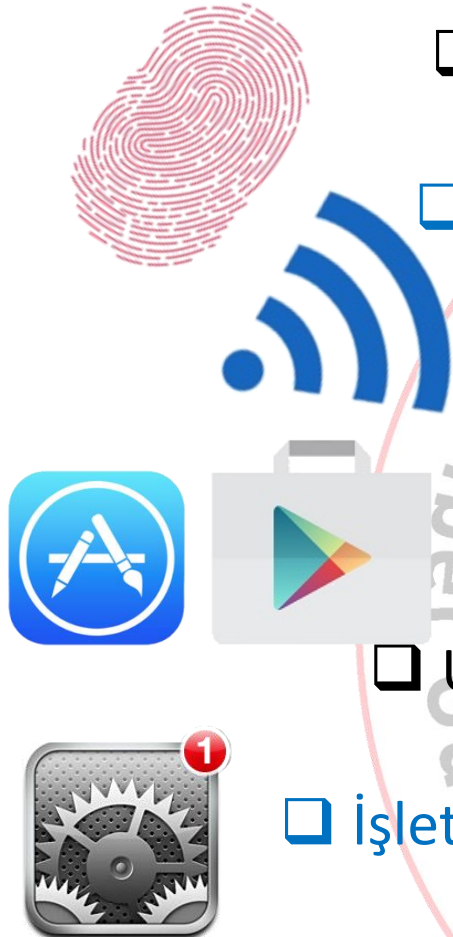
“Auto-lock” setting

Settings > Display & Brightness > Auto-lock (For iOS 9 and below: Settings > General > Auto-lock)
Set when you want your phone to auto-lock itself. The default is set to 5 minutes, but you can make it as low as 30 seconds.

5

Locked phone access setting

Settings > Touch ID & Passcode
Limit what your device can do while locked, like replying to messages or accessing your Apple wallet.



☐ 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!

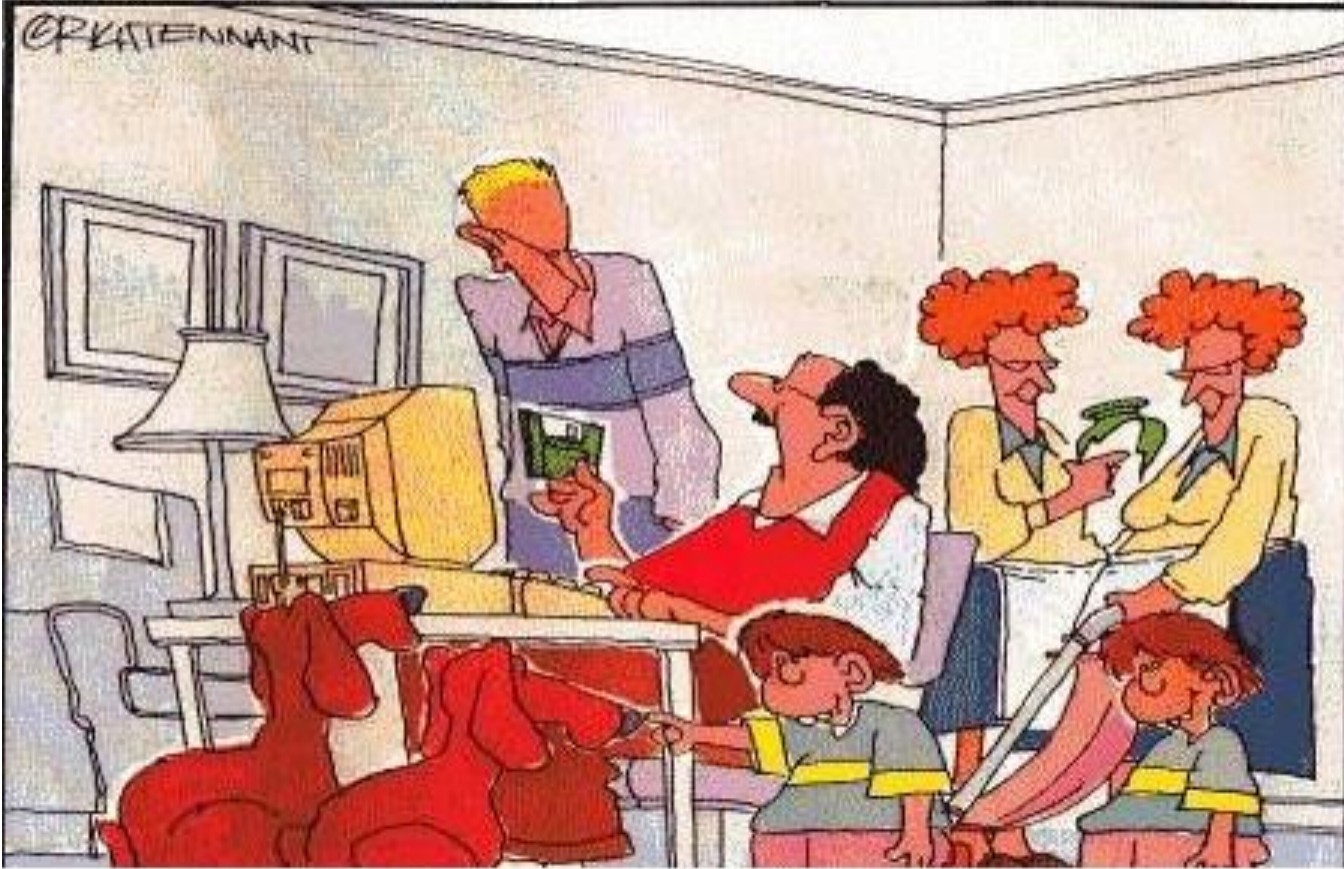
☐ İşletim sistemleri ve uygulamalar sürekli güncel tutulmalı!

☐ Cihazların satılmadan, teknik servise teslim edilmeden veya bir

başkasına verilmeden önce içeriği güvenli bir şekilde silinmelidir.

Yedekleme

SİBER GÜVENLİK
ENSTİTÜSÜ



Ben herşeyimi back-up'larım da...

gitim ve Ar



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

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



Bilgimi Koruyorum

► Bilgimi Koruyorum ► Ana Sayfa



**B!resi
biTgilerinizi
demiftirse**

**Öeler olupilix?
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 yabancı olmduğumuz 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

Ana Sayfa | Hakkımızda | TUBİTAK | BİLGEM

Google™ Özel Arama

Ara

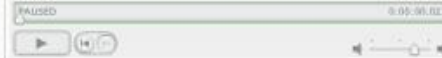
Konu Listesi / Menü

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

Sözlük

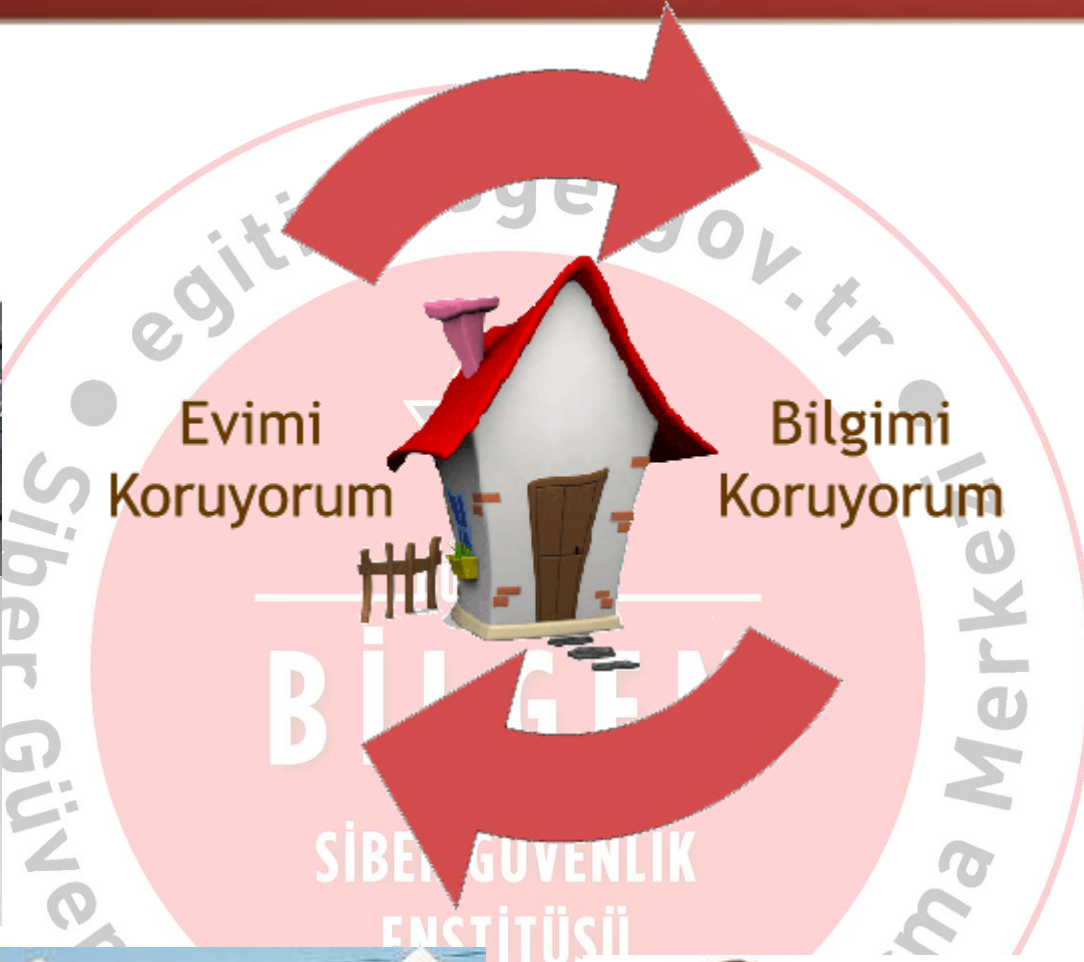


Bilgi Güvenliği Neden Önemli?



◀ Bilgimi Koruyorum

Eğitime Başlarken (Öneriler) ▶





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 yazılarınıza 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...

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

[Devamını oku...](#)

Duyurular

Siber Güvenlik Yaz Okulu 2014

p 2012 ve 2013 yıllarında Siber Güvenlik Yaz Kampı adıyla



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



Geleceğimiz için Güvenli Web



[İhbar Web](#) [Hakkımızda](#) [Sık Sorulan Sorular](#) [Site Haritası](#) [İletişim](#) [English](#)

Güncel Perşembe, 21 Ağustos 2014



Online Porno İzleme Yaşı Düştü

Bitdefender'in dünya genelinde 19 bin ebeveyn üzerinde yaptığı araştırmaya göre çocukların internet üzerinden porno içeriklere ulaşma yaşı 6'ya, internet üzerinden flört etme yaşı 8'e düşmüştür.

14
AĞUSTOS

[ARA](#)



DUYURULAR / ETKİNLİKLER

Tüm Duyurular

[İNTERNET İSTATİSTİKLERİ](#)

[ANKETLER](#)

[Oy Ver](#) [Sonuçları Gör](#)

[FAYDALI SİTELER](#)

[BİLİŞİM SÖZLÜĞÜ](#)


SEÇNEK ÇÖZÜMLERİ

AİLELER



İnternetin Güvenli Kullanımı için Anne-babalara Öneriler



EĞİTİMCİLER



Çocuklar İçin Güvenli İnternet Kullanımı E-kılavuzu



GÜVENLİK



İnternet Kafelerin Denetimi E-öğrenme Modülü



CC BY NC ND

111





Güvenli Çocuk Kulübü Açıldı

Sizin Görüşleriniz

cokkkkk güzel bir site herkeze tavsiye edrim hem sizde üye olun hadi durmayın hemen üye olunnnnnnnnnnn

gülşahfenerli

AĞUSTOS

21

0 Çevrimiçi

154 Ziyaretçi

Yeni Oyunlar



Yeni Üyeler



MÜHENDİS mühendiskerem İstanbul123 doktorsıla krprensos

Okul Ödevi

okulodevi.com

Gel ödevlerini beraber yapalım!



Öne Çıkanlar

! ?

bilmeceler



GUVENLIINTERNET.ORG

Çocukları Koruyun  Bilgisayarınızı Koruyun  İş Ve Özel Hayatınızı Koruyun 



Riskleri bilin önleminizi alın, Kendiniz ve sevdikleriniz için, “Güvenli İnternet” öğrenin!

Ebeveynler interneti öğrenecek

Aileler ve çocukların daha bilinçli bir bilgisayar ve internet kullanıcısı olmalarını amaçlayan "Bilgi Toplumunda Aile" eğitim seminerleri başlıyor. Seminere, HABERTÜRK de destek veriyor.

Microsoft Türkiye'nin aileler ve çocukların daha bilinçli bir bilgisayar ve internet kullanıcısı olmalarını amaçlayan "Bilgi Toplumunda Aile" eğitim seminerleri 24 Nisan pazar günü başlıyor. HABERTÜRK'ün de destek verdiğini seminerlerin ilki Microsoft Türkiye Ankara Ofisi'nin ev sahipliğinde gerçekleştirilecek. Seminerde, anne ve babalara bilgisayar ve internet konusunda bilgi verilecek. Çocuklar için de benzer amaca yönelik çalışmalar yapılacaktır.

"Bilgi Toplumunda Aile" seminerlerinin ailelere yönelik programı bilgisayar-çocuk-aile, bilgisayar ve video oyunları, sosyal paylaşım ağları ve bilgisayar güvenliği konularını kapsıyor. Eş zamanlı olarak çocuklara yönelik olarak verilecek eğitimlerde de bilgisayar ve internetin eğitim amaçlı kullanımı, bilgisayar ve video oyunları, sosyal paylaşım ağları ve çevrim içi oyunlarda güvenlik gibi konular ele alınacak. Microsoft Türkiye, konuyla ilgili açıklamasında, kurumsal sosyal sorumluluk vizyonuna işaret ederek, bu seminerlere ev sahipliği yapmaktan büyük memnuniyet duyduğunu belirtti.



Güvenli İnternet ifade paketi için tıklayın!





The screenshot shows the homepage of the stopthinkconnect.org website. At the top, there is a navigation bar with the text "STOP | THINK | CONNECT" and a tagline "Keeping the web a safer place for everyone." Below this is a menu with links: HOME, RESOURCES, CAMPAIGNS, GET INVOLVED, TIPS & ADVICE, and RESEARCH. The main content area has a dark blue background with a repeating pattern of small icons. A large white banner with green text reads "BE A GOOD CYBER CITIZEN BY OWNING YOUR ONLINE PRESENCE." Below this, the text "STOP. THINK. CONNECT." is displayed in large white letters. Underneath, there is a paragraph: "Take security precautions, understand the consequences of your actions and behaviors and enjoy the benefits of the Internet." This is followed by two sections: "STOP: Before you use the Internet, take time to understand the risks and learn how to spot potential problems." and "THINK: Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact your safety, or your family's." To the right, there is a large white text "DID YOU KNOW?" followed by a statistic: "28% of Americans say they lack knowledge about ways to stay safer online." At the bottom right, there is a Creative Commons license logo (CC BY NC ND) and the number "114".

STOP | THINK | CONNECT™ Keeping the web a safer place for everyone.

HOME RESOURCES CAMPAIGNS GET INVOLVED TIPS & ADVICE RESEARCH

**BE A GOOD CYBER CITIZEN BY
OWNING YOUR ONLINE PRESENCE.**

STOP. THINK. CONNECT.

Take security precautions, understand the consequences of your actions and behaviors and enjoy the benefits of the Internet.

STOP: Before you use the Internet, take time to understand the risks and learn how to spot potential problems.

THINK: Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact your safety, or your family's.

DID YOU KNOW?

28% of Americans say they lack knowledge about ways to stay safer online.

CC BY NC ND 114



[About](#) [Safer Internet Day](#) [Blog](#) [Events](#) [Research](#) [Get Involved](#)

[Advice Centre](#) [Hotline](#) [Helpline](#) [Pupil powered e-safety](#) [Q](#)

Announcing Safer Internet Day 2017

Together we reached 40% of UK children for #SID2016 - join us to make #SID2017 the biggest one yet!

Get Involved

Bilinçlendirme Posterleri

SİBER GÜVENLİK
ENSTİTÜSÜ

* * * * *
_ _ _ _ _

PAROLANI DEĞİŞTİRMEK
İÇİN SADECE
6
SAATİN VAR!

{ 8 karakterli bir parola 6 saatten az sürede kırılabılır }

KURUM_AL GÜV__LİK

S E N *'siz Olmaz!*

Poster - Sosyal Ağlar ve Siber Zorbalık



STOPTHINKCONNECT.ORG

Poster - Internet



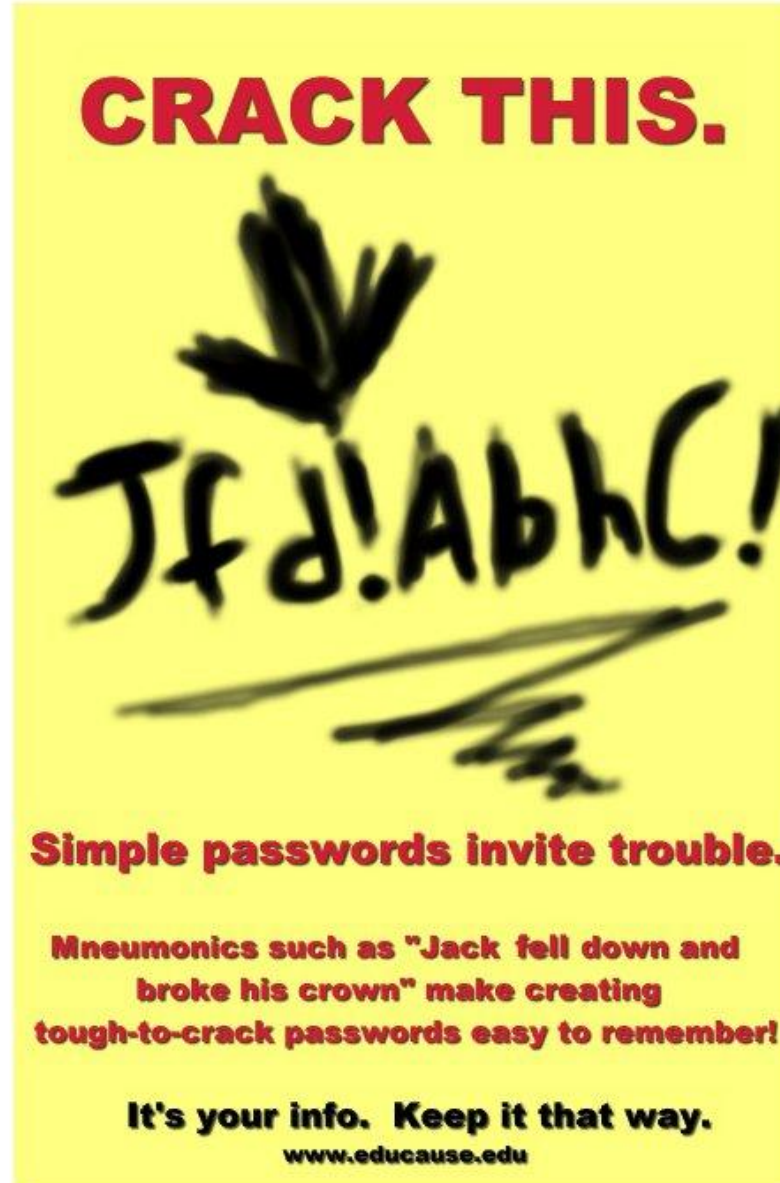
LOOKS can be **DECEIVING**...



Don't be **FOOLED**!
It might **DESTROY** you.

Make a move to **SAFEGUARD** your computers.

USE:
security updates
antivirus software
firewalls



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 ağınıza koruyun!
6. Evde kablosuz ağınıza (SSID) gizlemeyin!
7. İnternete bağlı cihaz almadan önce 2 kere düşünün!



- 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