Bilgi Güvenliği Farkındalık Eğitimi

2016 Ağustos

Bu sunu Bilgi Güvenliği AKADEMİSİ farkındalık eğitimlerinde kullanılan eğitim notlarının özeti niteliğindedir.

Detaylı içeriğe
http://www.slideshare.net/bgasecurity/bilgi-gvenlii-farkndalk-eitimi
adresinden ulaşabilirsiniz.

BGA Bilgi Güvenliği A.Ş

BGA Security Hakkında

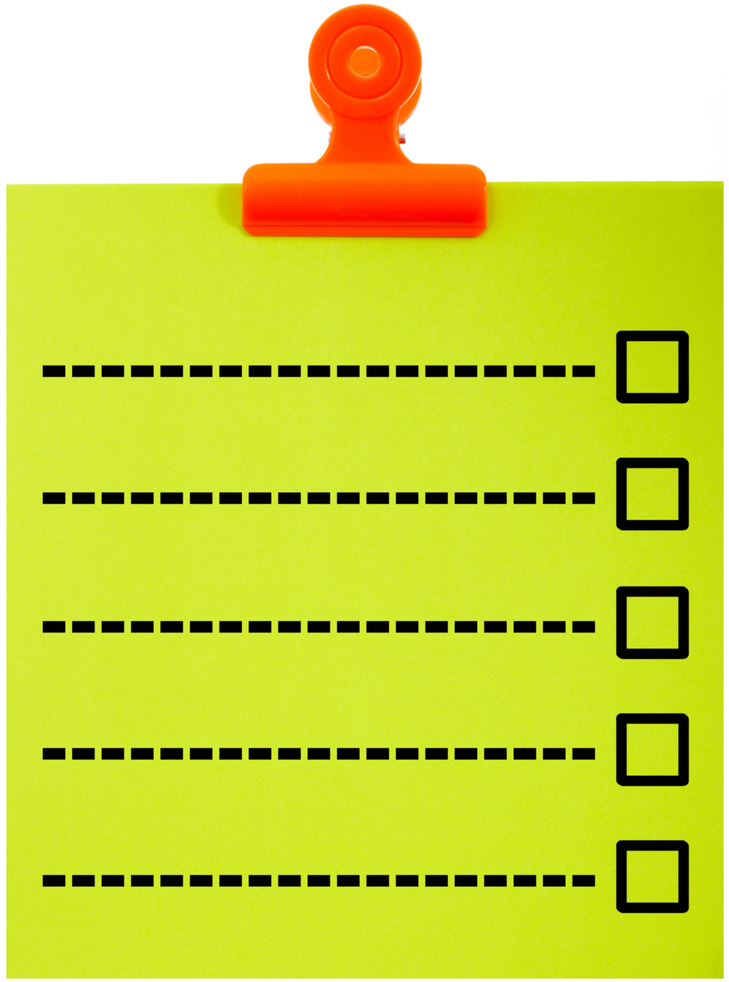
Siber güvenlik dünyasına yönelik, yenilikçi profesyonel çözümleri ile katkıda bulunmak amacı ile 2008 yılında kurulan BGA Bilgi Güvenliği A.Ş. stratejik siber güvenlik danışmanlığı ve güvenlik eğitimleri konularında büyük ölçekli çok sayıda kuruma hizmet vermektedir.

Gerçekleştirdiği vizyoner danışmanlık projeleri ve nitelikli eğitimleri ile sektörde saygın bir yer kazanan BGA Bilgi Güvenliği, kurulduğu günden bugüne kadar alanında lider finans, enerji, telekom ve kamu kuruluşları ile 1.000'den fazla eğitim ve danışmanlık projelerine imza atmıştır.

FARKINDALIK EĞİTİMİ

İÇERİK

- Bilgi Güvenliği Genel Kavramları
- Bilgi Güvenliği Önemi ve Tehditler
- Sosyal Mühendislik Saldırıları
- Sosyal Medya Riskleri ve Güvenlik
- Ağ Riskleri
- E-posta ve Mesajlaşma Güvenliği
- Parola Güvenliği
- Taşınabilir Bilgisayar ve Mobil Cihaz Güvenliği
- Fiziksel Güvenlik ve Veri Sızıntıları



KAVRAMLAR ve PRENSİPLER

BİLGİ GÜVENLİĞİ

Bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişim, kullanım, değiştirilme, ifşa edilme, ortadan kaldırılma, el değiştirme ve hasar verilmesini önlemek olarak tanımlanır ve “gizlilik”, “bütünlük” ve “erişilebilirlik” olarak isimlendirilen üç temel unsurdan meydana gelir.

Hangi bilgi bu kapsamdadır?

- Basılı halde kağıtlarda
- Telefon konuşmalarında
- Faks mesajlarında
- Masalarda, dolaplarda,
- İletim hatlarında,
- En önemlisi de kurum çalışanların zihinlerinde bulunur.

SİBER GÜVENLİK

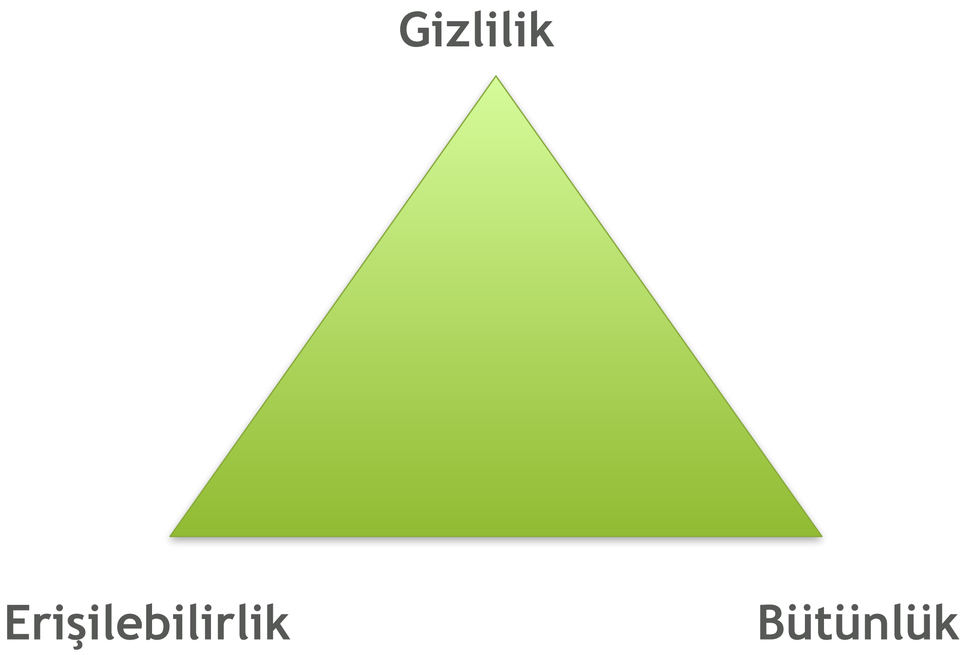
Manyetik ortamda bulunan ve iletişim halinde olan her bilginin güvenliği “Siber Güvenlik” kapsamında değerlendirilir.

Hangi bilgi bu kapsamdadır?

- Veritabanlarındaki
- USB / CD ‘ler
- Kişisel Bilgisayarlar
- Sunucular
- Cloud / Bulut çözümleri

Güvenli bir bilgi:

- Gizlidir,
- Bütündür,
- Erişilebilirdir.



BİLGİ GÜVENLİĞİNİN ÖNEMİ

KAVRAM VE PRENSİPLER

- Gizli bilgiler açığa çıkabilir.
- Bilginin içeriğinde yetkisiz kişiler tarafından değişiklikler yapılabilir
- Bilgiye erişim mümkün olmayabilir.
- Kuruma ait gizli ve hassas bilgiler ifşa olabilir
- Kurum işlerliğini sağlayan bilgi ve süreçler bozulabilir.
- Kurumun ismi, itibarı veya güvenilirliği zedelenebilir.
- Üçüncü şahıslar tarafından emanet edilen bilgiler zarar görebilir.
- Ticari, teknolojik, adli bilgiler zarar görebilir.
- İş sürekliliği zarar görebilir veya aksayabilir.

ÜLKEMİZDE BİLGİ GÜVENLİĞİ

KAVRAM VE PRENSİPLER

- Türkiye'de ise, en önemli gelişme 2013-2014 yıllarında ortaya çıkan Ulusal Siber Güvenlik Eylem Planıdır.
- Eylem planı, 2013 tarihinde resmi gazetede yayınlanarak yürürlüğe girmiştir.
- Özellikle kritik öneme sahip kurum ve kuruluşlara yapılması muhtemel saldırılara karşı önlem alınması planlanmaktadır.

SALDIRGAN AÇISINDAN

KAVRAM VE PRENSİPLER

- Bir sisteme sızmayı planlayan hackerin yapacağı ilk iş **düzenli bilgi toplama** ve değerlendirmedir.
- Bilgi toplama hacklemenin **ilk adımıdır** ve başarılı olması için gereklidir.
- Bilgi toplama esnasında bu gerekli mi değil mi diye sorulmadan alınabilecek **tüm bilgiler** toplanır.
- Toplanan bilgiler **sonraki aşamalarda kullanılmak üzere** sınıflandırılır.

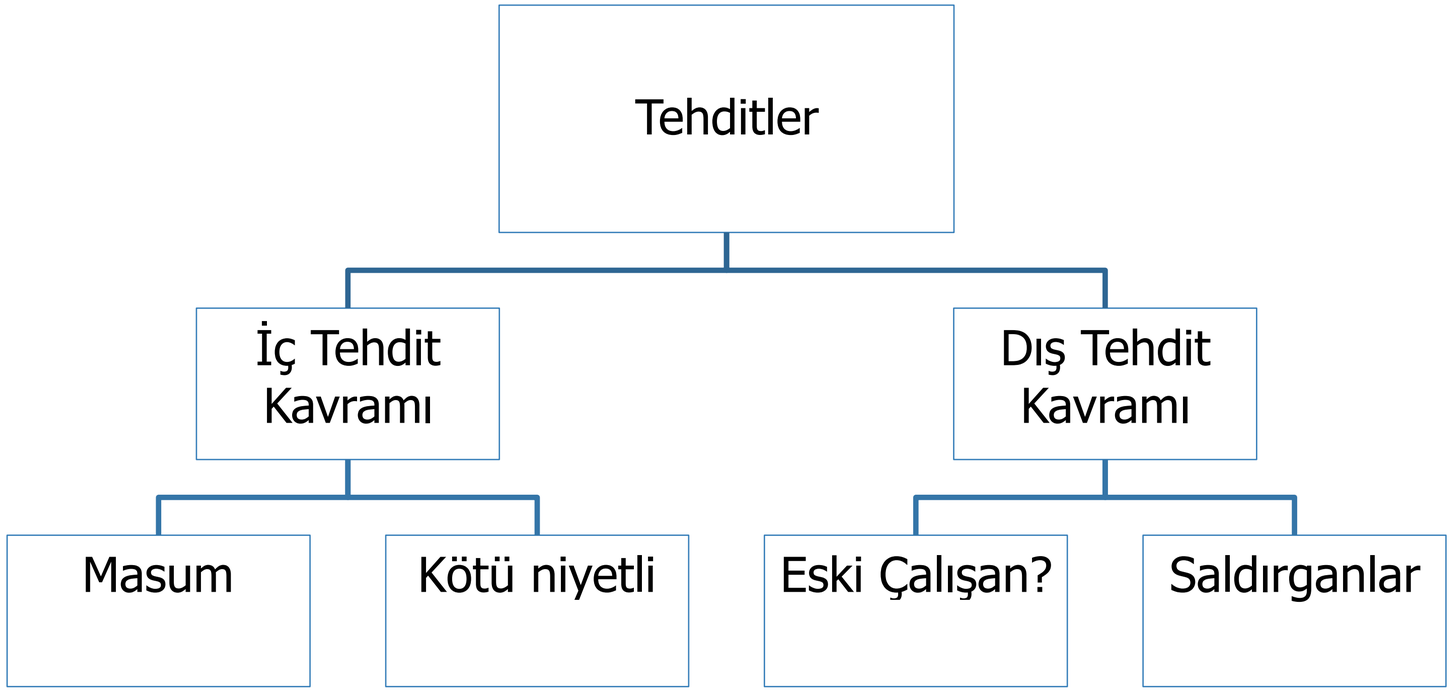
TEHDİTLER

BİLGİ GÜVENLİĞİNE YÖNELİK TEHDİTLER

TEHDİTLER

Siber Saldırılar; Kişi, Şirket veya Kurumun bilgi sistemlerine, iletişim altyapılarına yapılan planlı ve koordineli saldırılardır. Bu saldırılar ticari, askeri veya politik gibi amaçlar üzerine kurulabilir.

Siber Savaş; Yukarıda belirtmiş olduğumuz siber saldırıların Ülke veya Ülkelere yönelik yapılması duruma siber savaş tanımı getirilmiştir. Başta ABD ve Çin olmak üzere birçok ülke siber savaşlara karşı cephe kurmakta veya kurulmuş olan bu cepheleri güçlendirmeye çalışmaktadır.



İÇ TEHDİTLER

TEHDİTLER

- Bilgisiz ve bilinçsiz kullanım
- Temizlik görevlisinin sunucunun fişini çekmesi
- Eğitilmemiş bir çalışanın veri tabanını silmesi
- Kötü niyetli hareketler / firmaya zarar vermek
- İşten çıkarılan çalışanın, kuruma ait web sitesini değiştirmesi
- Bir çalışanın, ağda Sniffer çalıştırarak e-postaları okuması
- Bir yöneticinin, geliştirilen ürünün planını rakip kurumlara satması

DIŞ TEHDİTLER

TEHDİTLER

- Bir saldırganın kurum web sitesini değiştirmesi veya silmesi
- Bir saldırganın kurumun korunan bilgilerini çalması
- Bir saldırganın kurumun bilgilerini çalarak satması veya ifşa etmesi
- Birçok saldırganın kurum web sunucusunu servis dışı bırakma saldırısı yapması
- Yeni nesil APT (hedef odaklı) saldırıları

BİLGİ GÜVENLİĞİ TEHDİTLERİ

TEHDİTLER

- Sahtekarlık ve taklit,
- Kimlik hırsızlığı,
- Ticari bilgi çalma,
- İstihbarat amaçlı faaliyetler,
- Takip ve gözetleme,
- “Hack”leme, Defacement
- Virüsler, Truva atları…
- Casus yazılımlar (spyware),
- Spam ve benzeri saldırılar,
- Hizmet durduran saldırılar

ÖRNEKLER

SİBER SALDIRI İLE KAZANILAN SEÇİM

DÜNYA VE ÜLKEMİZDEN ÖRNEKLER

- Güney Kore’de muhafazakar iktidar partisi millet vekillerinden “Hong Joon-Pyo” seçimlerde hile karıştırdı.
- Yapılan seçimlere siber saldırı düzenlendi ve seçim hackerların müdahalesi ile kazanıldı.
- Bu durum sonrasında ortaya çıkınca istifa etmek zorunda kaldı.

ESTONYA SİBER SALDIRISI

DÜNYA VE ÜLKEMİZDEN ÖRNEKLER

- Rusya'nın bu ülkelere 2007 ve 2008 yıllarında saldırı yaptığı siber saldırılardır.
- Yapılan saldırılardan sonra ülkede bulunan resmi kuruluşların, finans ve basın-yayının bütün iletişimini haftalarca kesintiye uğrayarak milyonlarca dolar zarar verildi.
- Siber saldırıda, Estonya Cumhurbaşkanlığı, parlamento, birçok bakanlık siyasi partiler ve bankalarla diğer işletmelerin internet sitelerinin hedef alındığı, aşırı yüklenme nedeniyle ana sistemlerin çöktüğü ve ülkenin dış dünyayla bağlantısının kesilme noktasına geldiği belirtiliyor.
-

GÜRCİSTAN SİBER SALDIRISI

DÜNYA VE ÜLKEMİZDEN ÖRNEKLER

- Rusya’nın bu ülkelere 2007 ve 2008 yıllarında saldırı yaptığı belirtiliyor.
- Rusya, Gürcistan'a saldırmadan hemen önce Gürcistan iletişim altyapısının çökertilmesinden sorumludur.
- Savaştan önce tüm iletişim kanalları çökertildi ve ardından savaş başladı.
- Sıcak çatışmalara siber savaş unsurlarının da eşlik edeceğini kanıtladığını gördük..

ABD SİBER SALDIRISI - 2008

DÜNYA VE ÜLKEMİZDEN ÖRNEKLER

- Rusya’nın 2008 yılında ABD’ye yönelik yapığı saldırılar dikkat çekiyor.
- Virüslü bir hafıza kartıyla ABD’nin Irak ve Afganistan savaşlarını yürüten komuta merkezine sızmış ve ciddi sonuçlar alınmıştır.

BİR KLASİK - STUXNET

DÜNYA VE ÜLKEMİZDEN ÖRNEKLER

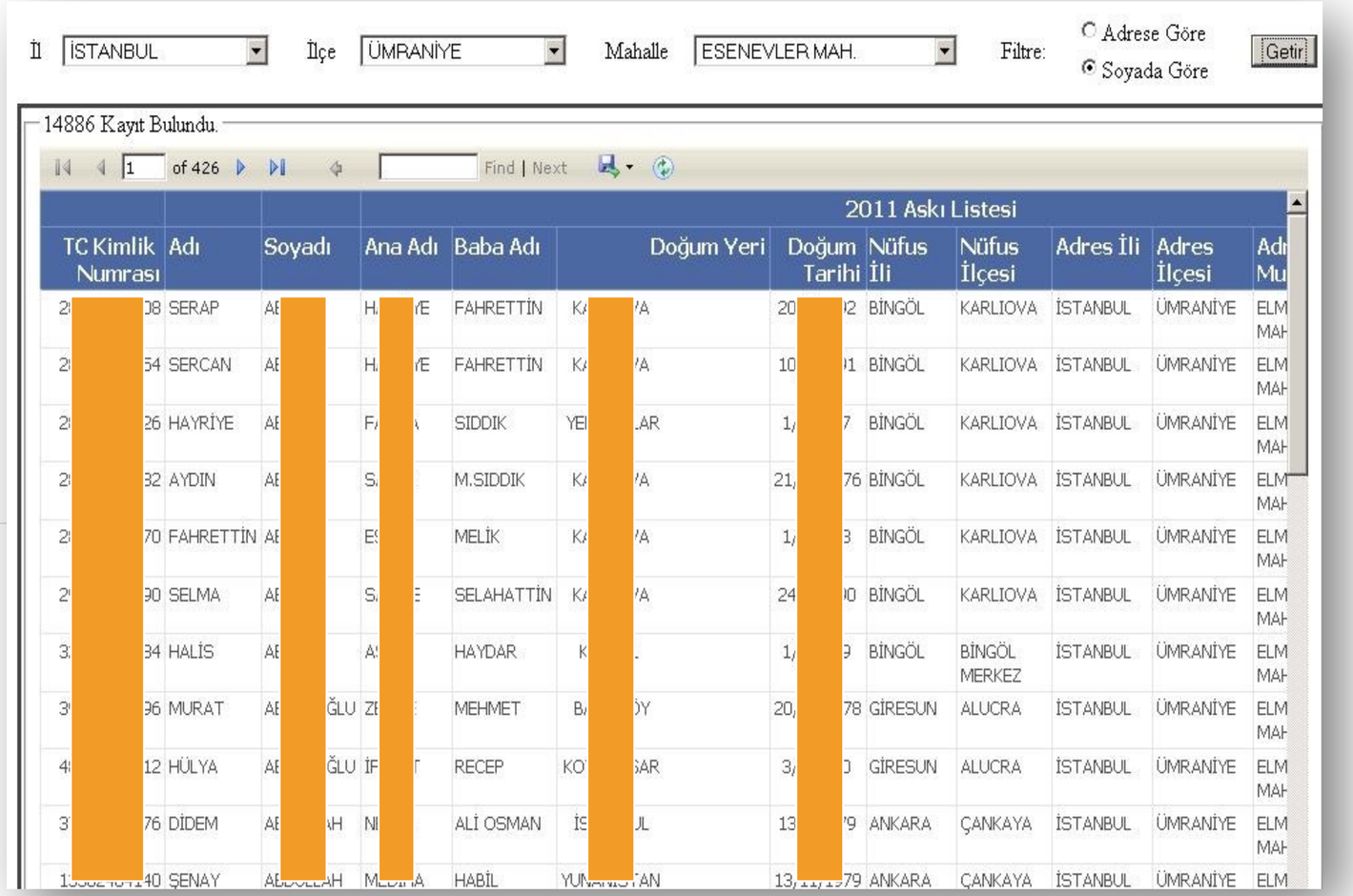
- Rusya, İran'ın nükleer programına sınırsız destek vermektedir. Rusya'ya karşı oldukça özgün bir taktik deneyen ABD kendi kendini kopyalayan bir yazılım olan Stuxnet virüsü ile saldırdı.

- Yazılım öncelikle motorları ve sıcaklığı kontrol eden merkezi mantık kontrol birimi olan PLC'yi ele geçirdi. Böylece sistemin kontrol eden diğer yazılımları da birer birer kolaylıkla elemine edebildi.

VATANDAŞLIK BİLGİLERİNİN SIZDIRILMASI - TR

DÜNYA VE ÜLKEMİZDEN ÖRNEKLER

- Geçtiğimiz seçimlerde bir siyasi partinin seçim sorgulama sistemine girildi.
- Bu sistem üzerindeki tüm data çalındı ve bir sorgulama yazılımı ile birlikte İnternet üzerinde hacker forumlarında dağıtıldı.



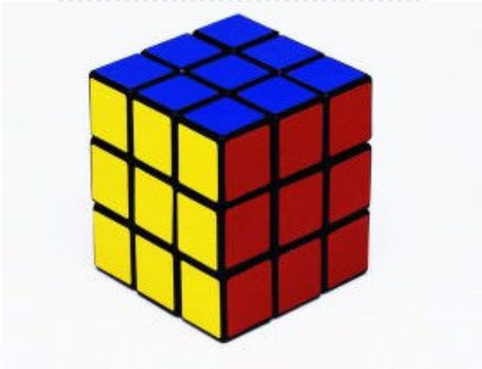
HACK VE HACKER KAVRAMI

HACK

HACK VE HACKER KAVRAMLARI

Hack

Kavramsal olarak bulunan bir materyal, alet, cihaz ya da nesneyi amacının haricinde kullanma işi HACKING olarak tanımlanır.



HACKER

HACK VE HACKER KAVRAMLARI

Hacker

Elektronik / mekanik herhangi bir nesneyi ya da cihazı maksadı dışında kullanmayı başarak kadar iyi kullanabilen kişilerdir.

Hacker günümüzde haberler, sosyal medya ve diğer platformlarda şifre, hesap çalma, sistem çökertme, zarar verme hatta bazen bankalardan para çalan kişilerin yaptığı hırsızlıklarla gündeme gelir

Tanıdığımız ilk hacker: Mac Gyver

NEDEN YAPILIR?

HACK VE HACKER KAVRAMLARI

Şantaj

Kişisel Tatmin

Bilgi

Hacking

Para

Politik sebepler

SOSYAL MÜHENDİSLİK VE BİREYSEL GÜVENLİK

BGA SECURITY

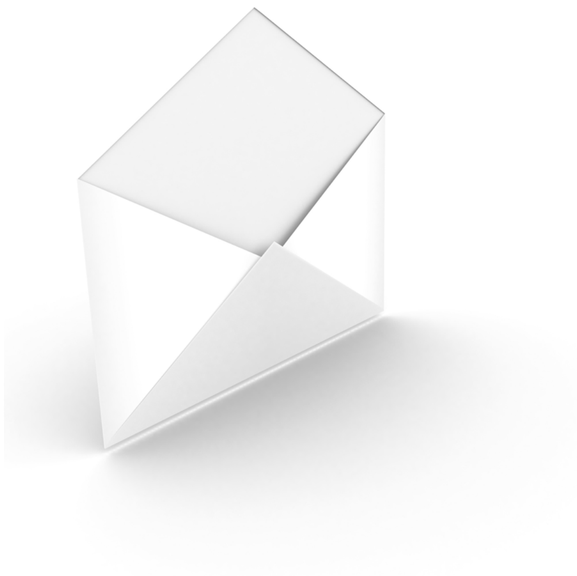
SOSYAL MÜHENDİSLİK SALDIRILARI

SOSYAL MÜHENDİSLİK

- Sosyal Mühendislik, insanlar arasındaki iletişimdeki ve **insan davranışındaki modelleri açıklıklar** olarak tanıyıp, bunlardan faydalanarak güvenlik süreçlerini atlatma yöntemine dayanan müdahalelere verilen isimdir.

- Kötü niyetli kişi, her konuşmada küçük bilgi parçaları elde etmeye çalışabilir. Konuşmalar daha çok arkadaş sohbeti şeklinde geçer. Bu konuşmalarda önemli kişilerin adları, önemli sunucu bilgisayarlar veya uygulamalar hakkında önemli bilgiler elde edilir.

- Sosyal Mühendislik için en etkin yol telefon ve e-postadır. Telefon haricinde kuruma misafir olarak gelen kötü niyetli kişiler bilgisayarların klavye veya ekran kenarlarına yapıştırılan kullanıcı adı ve şifre kağıtlarını da alabilirler. Çöplerinize kurumsal bilgi içeren kağıtlar atmayınız.



NASIL YAPILIR?

Bilgi Toplama
(Sosyal ağlar üzerinde etkilidir. Foursquare, Twitter, Facebook…)

İlişki Oluşturma
(Arkadaşlık talebi, sahte senaryolar üretilir, güvenilir bir kaynak olduğuna ikna edilir)

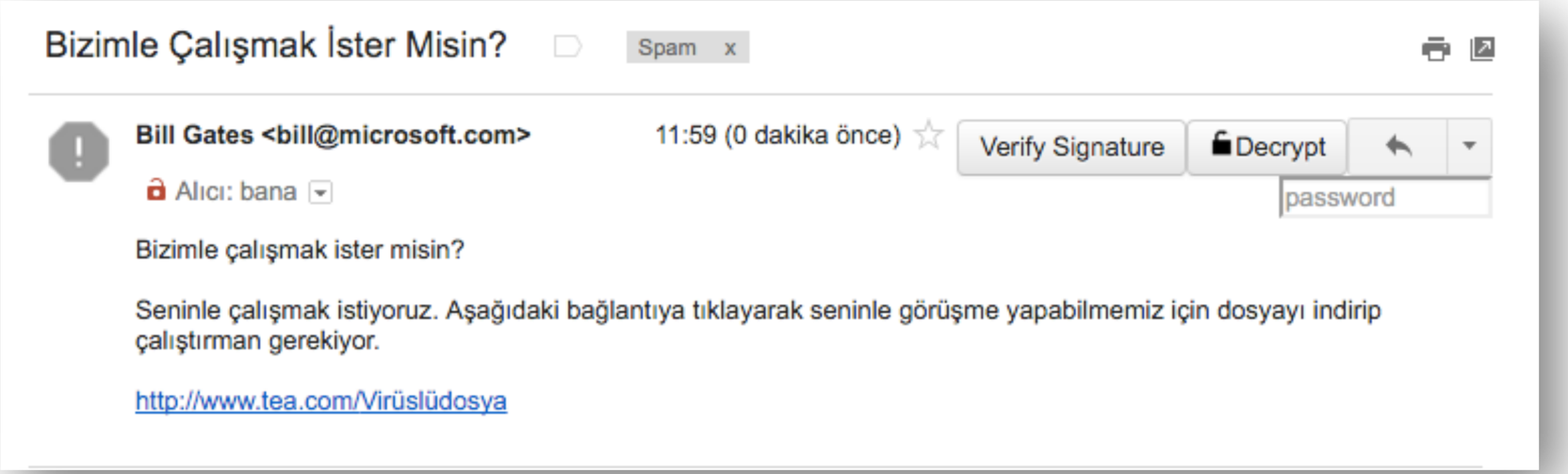
İstismar (Zararlı yazılımlar gönderilebilir)
Uygulama

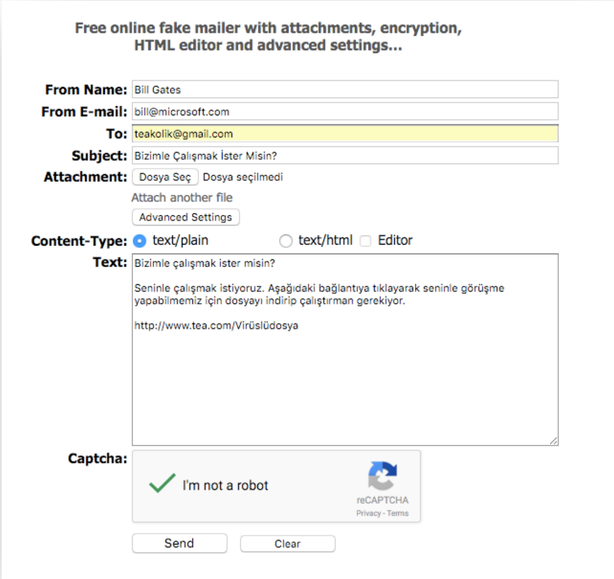
ÖNLEMLER

- Uygun olmayan yöntem ve kanallarla kurumsal bilgilerin **paylaşılmaması**
- Parola gizliliği prensibinin tüm **kurum genelinde** uygulanması
- **Parola paylaşımının** iş gereği olmaktan çıkması için alınacak diğer kontrol önlemleri
- Önemli durumlarda «**Geri Arama**» yönteminin tercih edilmesi
- Kurumsal gizlilik taşıyan evrakların uygun yöntemlerle **imhasının** sağlanması
- E-posta, posta ile gelen CD, yardımcı araç yazılımları **kullanımında dikkatli** olunması

SAHTE E-POSTALAR

SOSYAL MÜHENDİSLİK





PAROLALAR

SOSYAL MÜHENDİSLİK

Bilgisayarınızı korumak, **bilgisayar içinde sakladığınız bilgileri korumak adına** çok önemlidir. Bilgisayarınıza uzaktan ya da fiziksel olarak erişilebilir.

İzinsiz erişimi engellemek için bilgisayarınıza ve / veya işletim sistemine şifre tanımlamalı bilgisayarınızın başından kalkarken mutlaka oturumunuzu kilitlemelisiniz.

En önemli kişisel bilgi şifrenizdir.

- Herhangi bir şekilde paylaşılmamalıdır.
- Herhangi bir yere yazılmamalıdır.
- Yazılması gerekiyorsa güvenli bir yerde muhafaza edilmelidir.
- En az sekiz karakterli olmalıdır.
- Rakam ve özel karakterler (?, !, @ vs) içermelidir.
- Büyük ve küçük harf karakteri kullanılmalıdır.

PAROLA GÜVENLİĞİ

SOSYAL MÜHENDİSLİK

Dünyanın en büyük platformları hacklendi ve hacklenmeye devam ediyor. Bu sızmalar sonucunda uzmanlar kullanıcıların ne denli yanlış şifre tercihi yaptığını gözler önüne serdi.

Birçok kullanıcının güvenli olmayan şifre kullandığı görüldü. **12345678, Password*1** gibi kısa ve rutin şifrelerin çokluğu göze çarparken, bazı kullanıcıların her yerde farklı şifreyi hatırlamaktan endişe edercesine giriş yaptığı platformun adını kullandığı ortaya çıktı.

Uzun bir şifre, güçlü bir şifrenin başlangıcıdır. 10 ila 12 karakterli bir şifre iyi bir başlangıç olabilirken, banka gibi kritik sitelerdeki şifrelerin daha da uzun olmasında fayda var.

Geri dönüşüm iyidir ama şifreler için pek de iyi sayılmaz. Zira eninde sonunda daha önce sızmış bir şifre saldırganlar tarafından kullanılacaktır.

Her sitede aynı şifreyi kullanmamalısınız. Eğer bir sitede şifre saldırganların eline geçerse, diğerlerinde de geçmemesi için hiçbir sebep yok. – ki benzerlerini de görüyoruz

fuck	zzzzz	zzzz	zzz	xxxxx	xxxx
xxx	qqqqq	qqqq	qqq	aaaaa	aaaa
aaa	sql	file	web	foo	job
home	work	intranet	controller	killer	games
private	market	coffee	cookie	forever	freedom
student	account	academia	files	windows	monitor
unknown	anything	letitbe	letmein	domain	access
money	campus	explorer	exchange	customer	cluster
nobody	codeword	codename	changeme	desktop	security
secure	public	system	shadow	office	supervisor
superuser	share	super	secret	server	computer
owner	backup	database	lotus	oracle	business
manager	temporary	ihavenopass	nothing	nopassword	nopass
Internet	internet	example	sample	love123	boss123
work123	home123	mypc123	temp123	test123	qwe123
abc123	pw123	root123	pass123	pass12	pass1
admin123	admin12	admin1	password123	password12	password1
default	foobar	foofoo	temptemp	temp	testtest
test	rootroot	root	adminadmin	mypassword	mypass
pass	Login	login	Password	password	passwd
zxcvbn	zxcvb	zxccxz	zxcxz	qazwsxedc	qazwsx
qlw2e3	qweasdzxc	asdfgh	asdzxc	asddsa	asdsa
qweasd	qwerty	qweewq	qwewq	nimda	administrator
Admin	admin	alb2c3	lq2w3e	1234qwer	1234abcd
123asd	123qwe	123abc	123321	12321	123123
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		
55555	44444	33333	22222		
5555	4444	3333	2222		
555	444	333	222		
55	44	33	22		
5	4	3	2		

PAROLA GÜVENLİĞİ

SOSYAL MÜHENDİSLİK

“Forumlarda kullandığınız şifre eğer Hotmail’de kullandığınız şifre ile aynı ise, bir forum hack edildiği zaman aynı şifre olduğu için Hotmail hesabınızı da hack edebilirler.”

“Facebook’ta kullandığınız bir şifreyi Twitter’da kullanmak mantıklı olmayacaktır.”

Anlamlı birkaç kelime yerine dağınık kelimeler kullanın. Zira şifre “iyigünler” olduğunda yine saldırganların işi oldukça kolaylaşmış oluyor. Yaratıcı, kişisel ve elbette hatırlanabilecek birkaç kelime işinize yarayacaktır. Örneğin, “SeniSeviyorum” şeklinde alınan şifre yerine “MasaTopKavunKuzu” gibi bir şifre kullanmak daha etkili olacaktır.

“Unutmamak gerekiyor!

Güvenlikte en zayıf halka İNSANDIR!”

GÜÇLÜ PAROLA

SOSYAL MÜHENDİSLİK

“Peki Akılda Kalıcı Güçlü bir Şifre Nasıl Oluşturulur?”

Sevdiğinizin adı?	“**Ze**ynep”
Tuttuğunuz takım?	“**Ga**latasaray”
Doğum Tarihiniz?	“**19**80”

Şifreniz: **ZeGa19**

Daha güçlü: **!ZeGa19!**

Farklı Platformlar: **!ZeGa19!T** ***ZeGa19*F** **“ZeGa19”G**

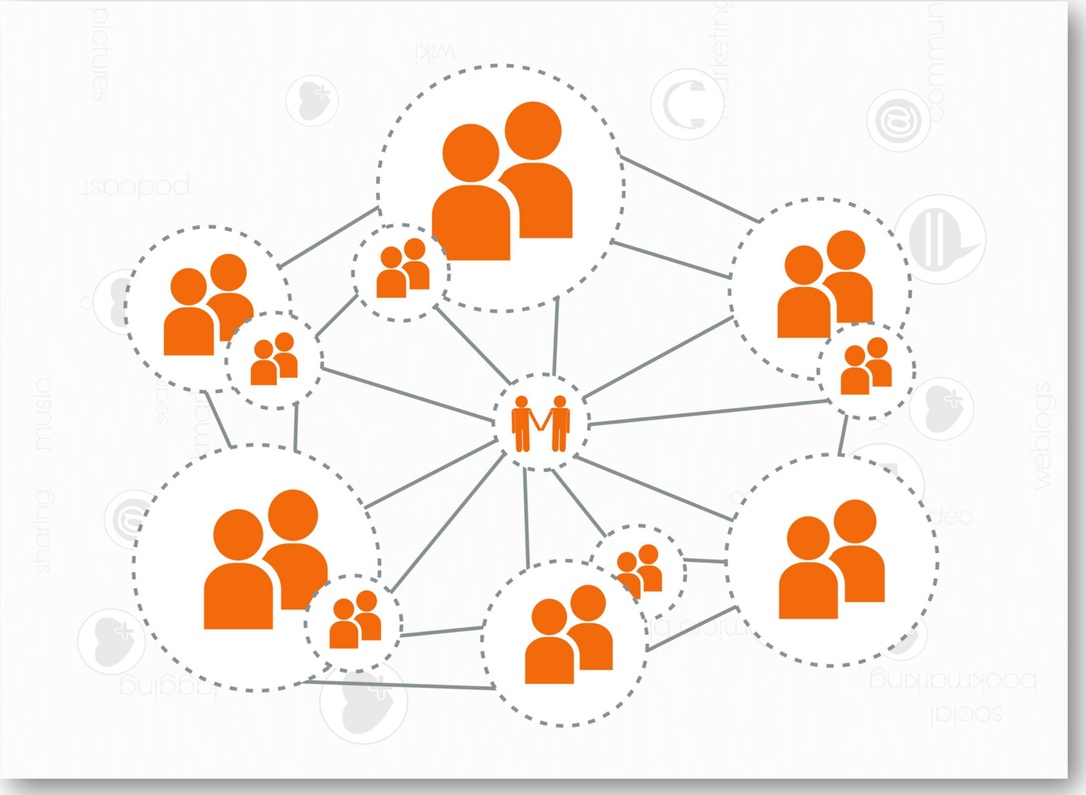
SOSYAL MEDYA

SOSYAL MÜHENDİSLİK

- Sosyal medya, Web 2.0'ın kullanıcı hizmetine sunulmasıyla birlikte, tek yönlü bilgi paylaşımından, çift taraflı ve eş zamanlı bilgi paylaşımına ulaşılmasını sağlayan medya sistemidir.

- Ayrıca sosyal medya; kişilerin internet üzerinde birbirleriyle yaptığı diyaloglar ve paylaşımların bütünüdür. Sosyal ağlar, insanların birbiriyle içerik ve bilgi paylaşmasını sağlayan internet siteleri ve uygulamalar sayesinde, herkes aradığı, ilgilendiği içeriklere ulaşabilirler.

- Gruplar arasında gerçekleşen diyaloglar ve paylaşımlar giderek, kullanıcı bazlı içerik üretimini giderek arttırmakta, amatör içerikler dijital dünyada **birer değer** haline dönüştürmektedir.



SOSYAL MEDYA RİSKLERİ

SOSYAL MÜHENDİSLİK

- Kurumsal hesabınız ele geçirilerek firmanız adına **olumsuz mesajlar** verilebilir.
- Güncelleme durumunuzdan **lokasyon tespiti** yapılabilir.
- Hesabınız kullanılarak yapınıza/şirket kurallarına **uygun olmayan yazılar** paylaşılabilir.
- E-posta vb gibi sistemlerin parolalarını resetlemek için gerekli gizli soruların cevabı bulunabilir.
- Çalıştığınız konum, iş arkadaşlarınız ve yöneticileriniz hakkında bilgi edinilebilir
- Instagram, Facebook, Twitter, Linkedin ve son olarak icloud ciddi güvenlik riskleri yaşadı.
- Kullanıcıların elinde olmayan tamamen bu tarz güvenlik risklerini unutmayın!
- Paylaşımlarınıza bir sınırlama getirin ve kurtarma senaryolarına hazırlıklı olun !

GÜNLÜK YAŞAM RİSKLERİ

SOSYAL MÜHENDİSLİK

İnternetten telefon sipariş etti, gelen kutudan salatalık çıktı

Bir internet sitesinden cep telefonu siparişi veren Yusuf Kumaz'a gelen kutudan, oyuncak bir telefon ve küçük bir salatalık çıktı.

Eklenme: **25 Ocak 2014 14:23** / Güncelleme: **25 Ocak 2014 14:35** / **44,455** Okunma / **10** Yorum

SOSYAL AĞ RİSKLERİ

SOSYAL MÜHENDİSLİK

xxBank

Sayin XX Bank Musterisi

Hesabiniza 24/subat/2005 tarihinde Huseyin Abacioglu tarafindan 270 YTL. havale edilmistir. Yapilan havale ile ilgili ayrintilar asagidadir.

Gonderen: Huseyin ABACIOGLU
Miktar: 270,00 YTL. (iki yuz yetmis yeni turk lirasi)
Sube: Mardin / Merkez
Aciklama: -

Havale onay ve/veya red islemi icin asagidaki linkden internet bankaciligini kullanabilirsiniz ve/veya hesabinizda gerekli incelemeleri yapabilirsiniz. Size havale gonderen kisinin bilgileri icinde asagidaki linki kullanabilirsiniz...

https://secure.XX.com.tr/isube/login.jsp?islemno=SD893RGSFCV783C&ssl=1&isube=active&system=93 (**Lutfen buraya tiklayin...**)

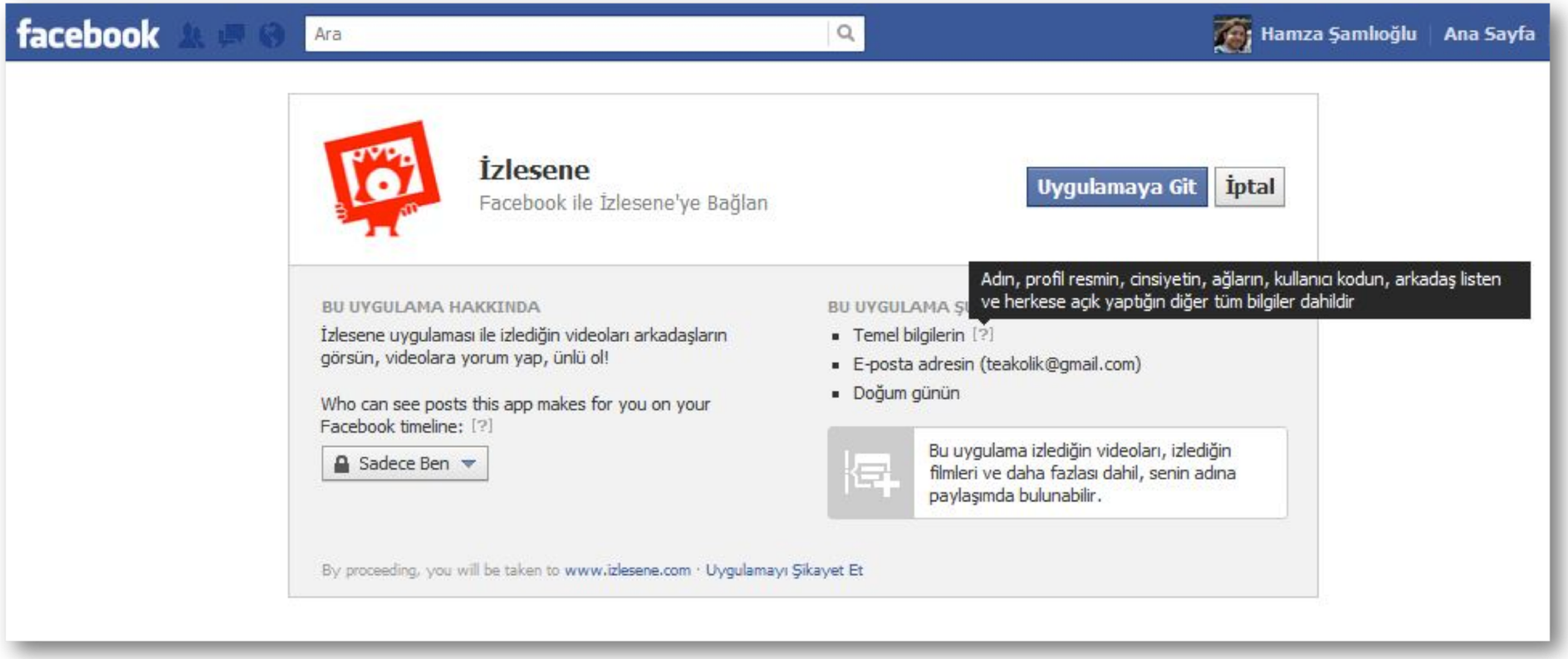
Ebru Polat 30 Ekim, 17:03 Şikayet Et

iyi günler,
bir bayan olarak söyleme ihtiyacı durumundayım,şurada bir bayanın çıplak görüntüleri var ve aşağılıkça bir video
ben şikayet ettim,sizi neden ilgilendirdiğine gelince videonun altında sizin email adresiniz yazıyor ve kimlik bilgileriniz var videodaki bayan sizin arkadaşınızmış şeklinde bir yazı yazılmıs adres
www.facabook.com/video/video/video.php?v=1381831528939 60

Sahte Adres:
www.facabook.com

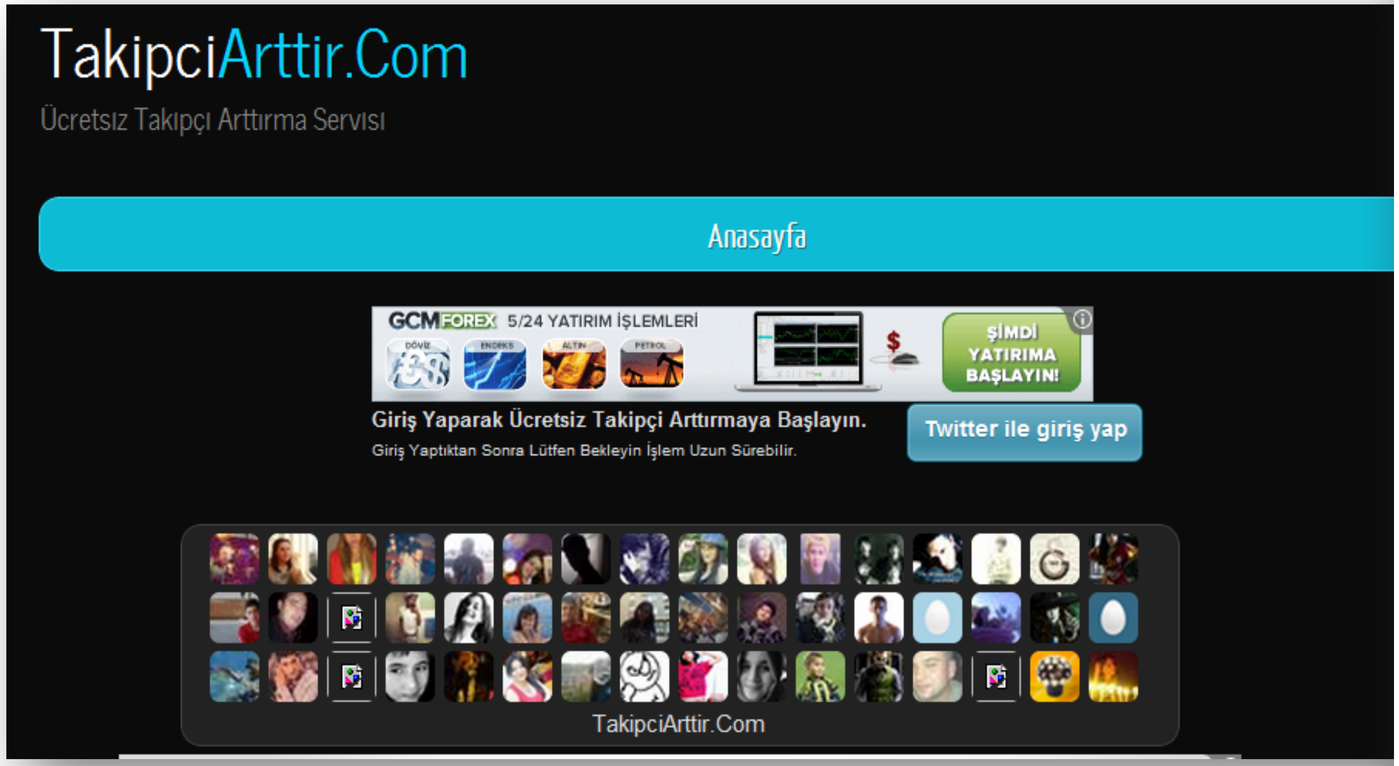
SOSYAL AĞ RİSKLERİ

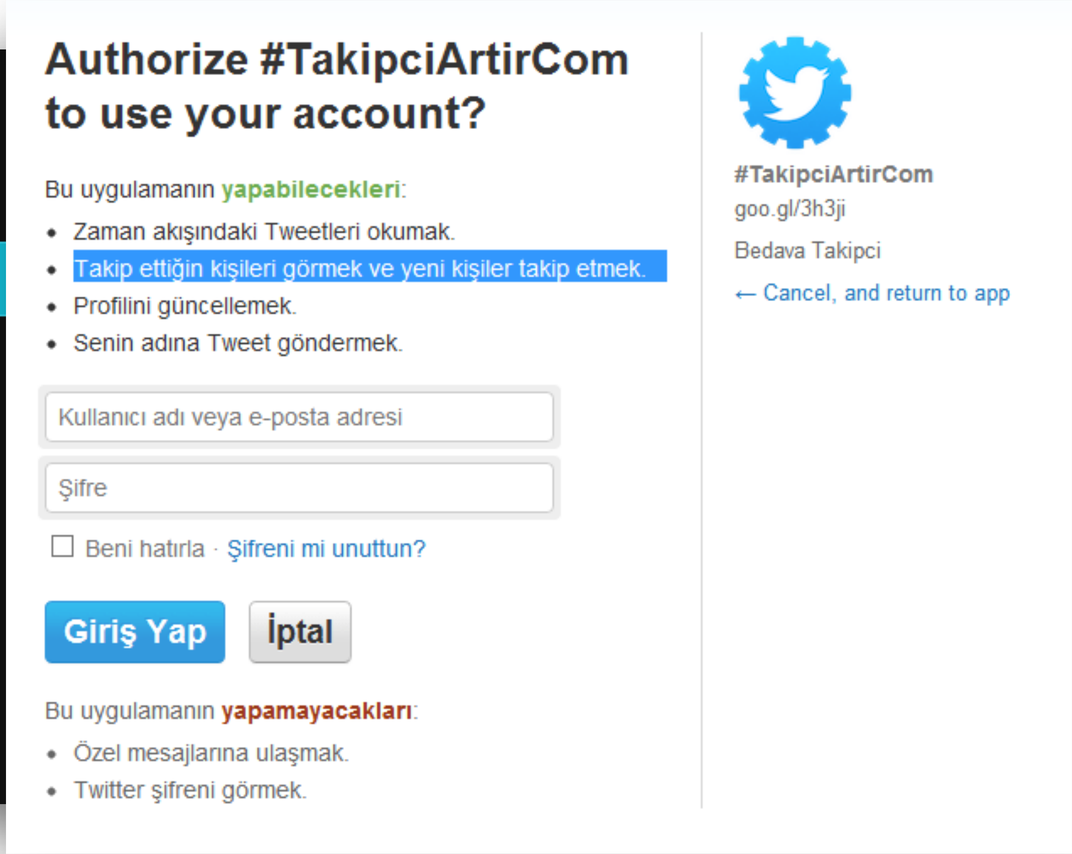
SOSYAL MÜHENDİSLİK



SOSYAL AĞ RİSKLERİ

SOSYAL MÜHENDİSLİK





UNUTMAYIN!

SOSYAL MÜHENDİSLİK

- Sahte Hesaplara Dikkat!
- Sahte Haberlere Dikkat!
- Oltalama saldırılarına karşı dikkat!
- Casus yazılım bulaştırma senaryolara karşı dikkat!
- Crackli uygulamalar kullanmayın!
- Sosyal Medya hesaplarına güvenli erişim!
- Hesabın ele geçirilmesine karşı önlemler alın!

YAPMAYIN!

SOSYAL MÜHENDİSLİK

- Sosyal ağlarda **ÖZEL veya ŞİRKET** bilgilerini paylaşmayınız
- Güvenmediğiniz kaynaklardan bildirilen uygulamaları Facebook hesabınızda kullanmayınız,
- Kişisel bilgilerinizin çalınmasına ve dolandırıcılık uygulamalarına alet olmanıza sebep olabilir
- Güvenmediğiniz linklere tıklamayınız ve uygulamalara erişim izni vermeyiniz
- Arkadaşınızdan gelen genellikle bozuk bir dille yazılmış (otomatik çevirmen yazılımları ile çevrilmiş) mesajlar ve linkler
- Mesaj içinde çok dikkat çekici ifadelerin kullanımı (skandal, en iyiler vs.)
- Kullandığınız uygulamalar arasında güvenmedikleriniz varsa kaldırın

İKİ ADIMLI DOĞRULAMA

SOSYAL MÜHENDİSLİK

- İki aşamalı kimlik doğrulamayı aktif edin.
- Parolanız, e-posta adresiniz ele geçirilse bile saldırganın hesabına erişmesini yada hesap bilgilerinizi değiştirmesini engellemek için telefon onay kodu ile hesabınızı koruyabilirsiniz.

“Bankacılık sistemlerinde olduğu gibi” ücretsiz olarak sunulur!

- Her girişte sms almamak için güvenli bilgisayar yada güvenli browser tanımlaması yapabilirsiniz.
- Gmail, Apple, Twitter, Facebook, Linkedin vb. platformlar destekler.

AĞ GÜVENLİĞİ

KABLOSUZ AĞLAR

AĞ GÜVENLİĞİ

KAMUYA AÇIK KABLOSUZ AĞLARA DİKKAT!

Tren, Havaalanı, Gemi, Otobüs, Ev, İş, Kafe, Otel, Restorant…

Ortak kablosuz ağlar veya parola korumasız ücretsiz kablosuz ağlarda **VERİLERİNİZİN İZLENMESİ** riski yüksektir.

Kritik işlerimlerinizi güvenli olmadığını düşündüğümüz kamuya açık kablosuz ağlar üzerinden yapmayın.

HTTP / HTTPS KAVRAMLARI

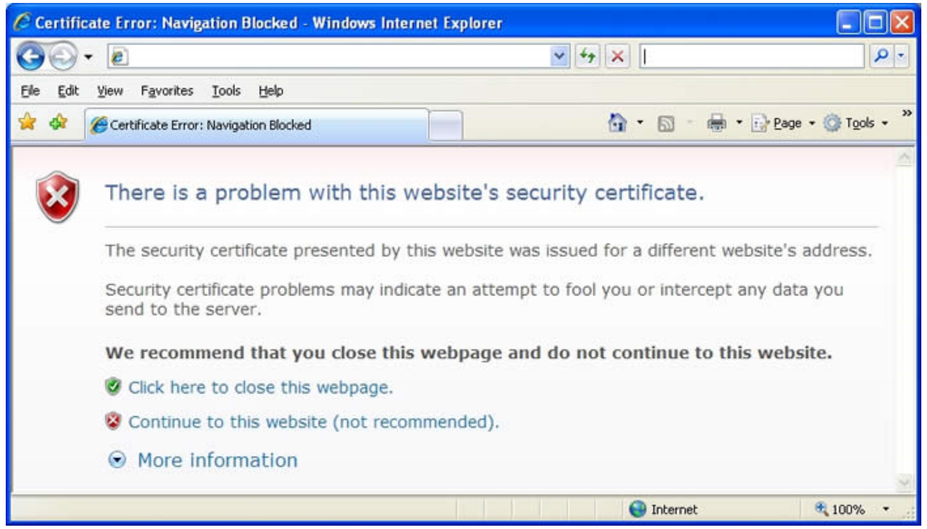
AĞ GÜVENLİĞİ

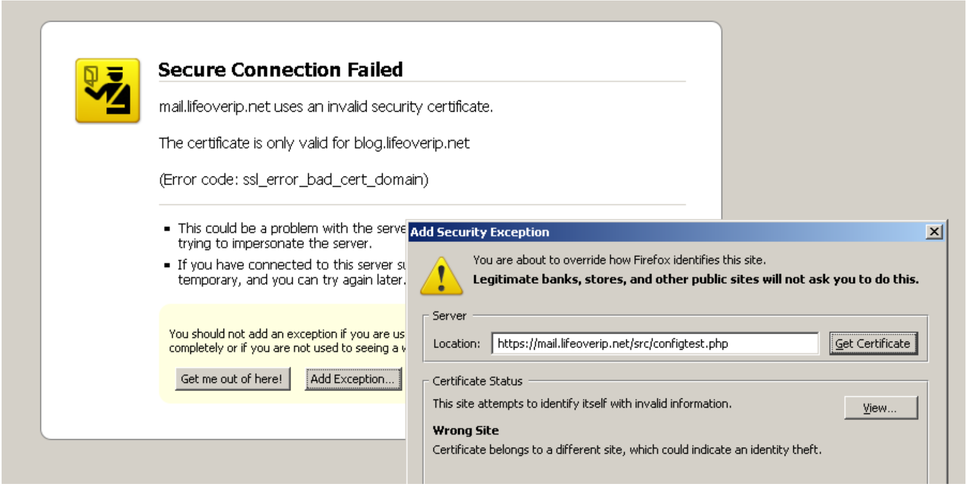
- **http://** Hyper-Text Transfer Protocol, Türkçe Hiper-Metin Transfer Protokolü bir kaynaktan dağıtılan ve ortak kullanıma açık olan hiper ortam bilgi sistemleri için uygulama seviyesinde bir iletişim kuralıdır. 1990 yılından beri aktif olarak kullanılmaktadır.

- **https://** Netscape tarafından 1994 yılında geliştirilen Secure Sockets Layer (Güvenli Giriş Katmanı) protokolü, internet üzerinden güvenli veri iletişimi sağlayan bir protokoldür.

- Yerini yavaş yavaş TLS 1.3'e bırakmış olsa da SSL 3.0 günümüzde tüm internet tarayıcıları tarafından desteklenmektedir.

- HTTP man-in-the-middle attack, yani ortadaki adam saldırısına ve dinlemelere karşı korumasızdır. Ağı dinleyerek verileri toplayan bir saldırgan kolaylıkla bilgileri okuyabilir ve gizli kalması gereken parolaları, kullanıcı hesaplarını ele geçirebilir. HTTPS ise bu tür saldırılardan korunmak amacıyla tasarlanmıştır. Bu nedenle HTTPS, çoğunlukla parola ve kullanıcı adlarının gönderildiği form sayfalarında tercih edilir. Tamamen HTTPS ile yayın yapan web siteleri de mevcuttur.





e-posta GÜVENLİĞİ

AĞ GÜVENLİĞİ

- Bugün hala en populer saldırı vektörü e-postalardır,
- Zararlı yazılımların en kolay bulaşma vektörü e-postalardır,
- E-postaların geldiği adreslere dikkat edilmelidir,
- Şüpheli e-posta ekleri ve linkleri için bilgi işlem departmanına başvurun,
- Epostalarda gizli bilgi asla göndermeyin

Neden eposta?

Son kullanıcıya ulaşmanın en kolay ve maliyetsiz yoludur.

MOBİL GÜVENLİK

BGA SECURITY

BAKIŞ

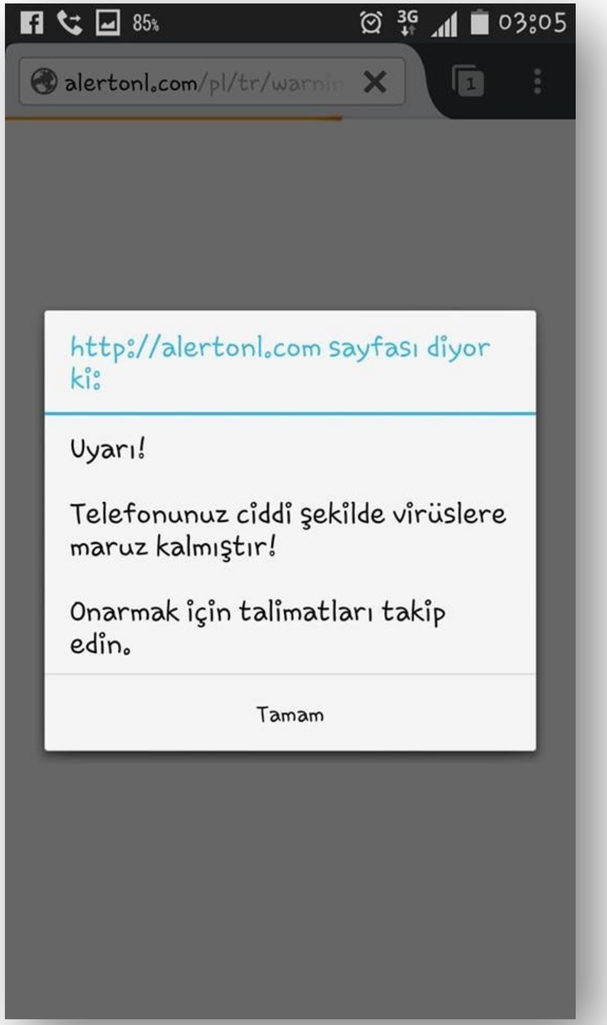
MOBİL GÜVENLİK

Akıllı telefonlar ve günümü teknoloji dünyası sebebi ile her birimiz birer “Online” bireyler haline geldik. Online kalmak zorundayız!

Peki Mobil Cihazlarımız Güvenli mi?

Akıllı telefonlar zararlı yazılımlar ile kontrol altına alınabilir.

- Sms geçmişi
- Yer Tespiti
- Arama geçmişi
- Mesajlaşma uygulamaları
- İzinsiz arama
- Hassas bilgilere erişim
- Gizli fotoğraf çekme
- Ortam dinleme…



MOBİL İŞLETİM SİSTEMLERİ

MOBİL GÜVENLİK

- Android
- iPhone
- Windows Mobile
- Diğerleri…

VARSAYIMSAL RİSKLER

TAKİP EDİLİYORUZ!

Mobil sistemlerin yaygınlaşması ve akıllı cep telefonlarının yoğun kullanımı, hackerların dikkatini bu yöne doğru çekiyor.

Akıllı telefonlar, klasik bilgisayar sistemleri ile yapılabilen her şeyi yapmak üzere geliştirildiği için riskler de o oranda artmıştır.

iPhone ve iPad 3G Her Hareketinizi ve Her Çağrınızı Takip Ediyor

Apple'dan sevgilerle: "Her Hareketinizi ve Çağrınızı İzliyoruz"! Tüm dünya bugün (20.04.11) California Santa Clara'da düzenlenen "**Where 2.0**" 2011 konferansında *Alasdair Allan* ve *Pete Warden* adlı araştırmacıların **iPhone** cep telefonunun ve **iPad 3G** mobil cihazının kullanıcıların her hareketini gizli br dosyada kaydettiğini açıklamasıyla sarsıldı. Peki bu nasıl gerçekleşiyor ve Apple'ın derdi ne?

iPhone ve iPad Verilerine Uzaktan Erişilebiliyor

Elcomsoft Phone Password Breaker isimli bir adli bilişim aracı, iPhone ve iPad'lerin tüm verilerine cihazla herhangi bir fiziki temasa girmeden gerçek zamanlı olarak erişebiliyor. Böylelikle adli bilişim işlerini oldukça kolaylaştırıyor. Tabi bunun yanında eğer isterse bütün verilere her daim ulaşabiliyor. Araç, iPhone ve iPad'ini yedeklemek için **iCloud**'u kullanan ürün sahiplerini hedef alıyor.

MOBİL İLETİŞİM GÜVENLİĞİ

MOBİL GÜVENLİK

- Sahte aramalara dikkat!
- Kurulan yazılımların kullanmaları gereken kaynaktan fazlasına erişim istemesi
- Arka planda çalışan yazılım ve servislerin izlenmesi
- Güvenlik ayarlarında bilinmeyen kaynaktan yazılım yüklenmesine engel olmak
- Mobil anti virüs kullanmak periyodik tarama yapmak, gereksiz veya güvenilmeyen uygulamaları kaldırmak
- Mobil cihaz yönetim yazılımı kullanmak
- İşletim sistemini güncel tutmak
- Market üzerinde uygulama yayıncısını doğrulamak

Kurumsal bilgileri ve parolaları mobil sistemlerde şifreli olarak tutulmalı!

MOBİL BİLGİSAYARLAR

MOBİL GÜVENLİK

- Gerekli olmadıkça «Admin» yetkisinin kullanılmaması
- Kurum dışında kullanım kurum güvenlik politikalarına uyulması
- Kablosuz ağ kullanılmıyorsa Wifi mutlaka kapalı tutulmalı
- Güvenlik duvarı kapatılmamalı
- İşletim sistemi yamaları yüklenmeli
- Antivirüs kurulmalı ve açık kalmalı
- Taşınabilir bilgisayarla kurum dışına çıkan bilginin güvenliği için uygun şifreleme yöntemleri kullanılmalı
- Dizüstü bilgisayarlarda özel bilgi işyeri bilgisi ayrımı yapılmalı

Komuta kodları çalındı

ABD Ulusal Havacılık ve Uzay Dairesi'nden (NASA) geçtiğimiz yıl çalınan bir diz üstü bilgisayarda Uluslararası Uzay İstasyonu'nun komuta kodlarının yer aldığı açıklandı. NASA bilgisayarları ve mobil cihazlarının sadece yüzde 1'indi şifre olduğu öğrenildi.

Güncelleme: 12:41 TSİ 01 Mart. 2012 Perşembe

NASA Genel Müfettişi Paul Martin, ISS komuta algoritmalarını içeren diz üstü bilgisayarın 5 Mart 2011 tarihinde çalındığını ve şifresinin bulunmadığını söyledi. Martin, 2011'de yaşanan kötü amaçlı yazılım saldırısı ve güvenlik ihlali sayısının 5,408 olduğunu belirtti.

ABD Temsilciler Meclisi'ne verilen raporda, çalınan diğer diz üstü bilgisayarlardan birinin, gelecekte insanlı uzay uçuşları için geliştirilen Çok Amaçlı Mürettebat Aracı (MPVC) projesiyle ilgili bilgiler içerdiği ifade edildi. Ayrıca, Nisan 2009 ile Nisan 2011 arasında 48 mobil cihazın çalındığı bilgisi verildi.

SAHTE ARAMALAR

MOBİL GÜVENLİK

İnternet dünyasının sağladığı özgürlüklerden faydalanan saldırganlar, siber casusluk, şantaj ve benzeri siber suçlar için sahte aramalar gerçekleştiriyor.

SIP/VOIP ilişkisi

Sahte arama yapan servislere örnek!

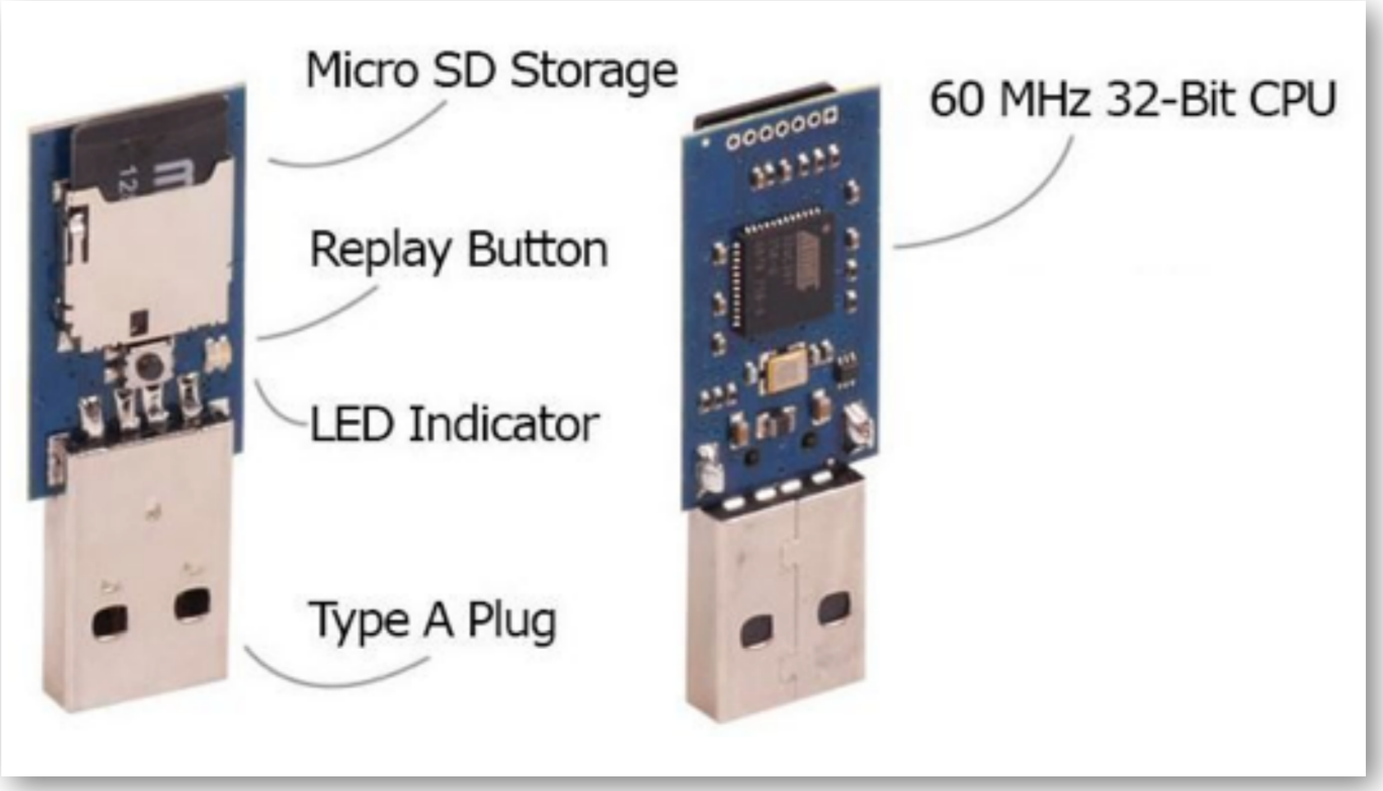
12voip.com
Calleridfaker.com

HID AYGITLARI

MOBİL GÜVENLİK

USB Rubber Ducky klavye chipsetine sahip programlanabilir konsept bir donanımdır.

USB Rubber Ducky aynı zamanda içinde bulunan micro sd kart ile sisteme veri aktarabilme özelliğine de sahiptir.



HID AYGITLAR - RUBBER DUCKY

MOBİL GÜVENLİK

- USB portundan erişim kurduğunuz tüm sistemlerde,
- Linux / Windows / Mac OS X işletimi sistemine sahip tüm bilgisayarlarda
- Micro Usb Girişe Sahip Mobile Cihazlar (Android vb.)
- Switch/Router gibi aktif ağ cihazları
- Endüstriyel Sistemler

Zigbee CC2531 USB dongle sniffers sniff yakalandı CC2650 protokol analizörü

US $14.99 / parça

Min. Sipariş: **1 parça**

Sylvia store

Ücretsiz kargo! 1 adet cc2531 usb dongle f256 protokol analizörü ethereal paket dinleyicisi

US $28.80 / parça

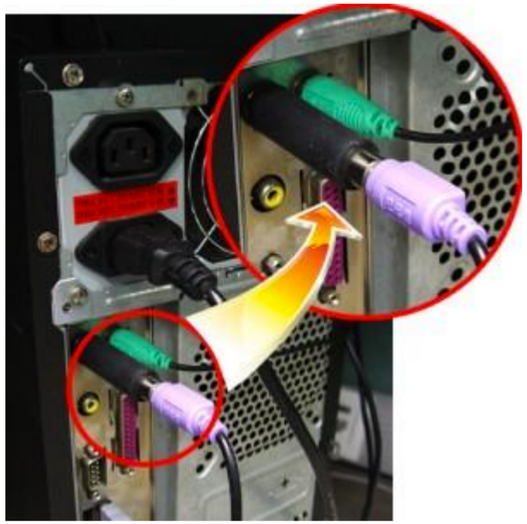
Min. Sipariş: **1 parça**

Super Electric modules Market

KEYLOGGERLAR

MOBİL GÜVENLİK

- Klavye girişlerini hafızasına kaydeder.
- Kablosuz ağ üzerinden veri aktarma özelliğine sahip modelleri vardır.



ÖNERİLER

MOBİL GÜVENLİK

- Kurumsal ve kişisel güvenlik duvarları kullanılmalı
- Güncel işletim sistemleri ve browser kullanılmalı
- Browser yazılımları sıkılaştırılmalı
- Browser yazılımları uyarılarına dikkat edilmeli parolalar kaydedilmemelidir
- Kurumsal, merkezi yönetilen anti virüs yazılımı kullanılmalı
- Anti spyware veya internet güvenlik yazılımı kullanılmalı

YASALAR

- 5651, 5070 ve 5846 Sayılı Kanunlar
- TCK Madde 135 (Kişisel verilerin kaydedilmesi)
- TCK Madde 136 (Verileri hukuka aykırı olarak verme veya ele geçirme)
- TCK Madde 243 (Bilişim sistemine grime)
- TCK Madde 244 (Sistemi engelleme, bozma, verileri yok etme veya değiştirme)
- TCK Madde 326 (Devletin güvenliğine ilişkin belgeler)
- TCK Madde 327 (Devletin güvenliğine ilişkin bilgileri temin etme)
- TCK Madde 328 (Siyasal veya askeri casusluk)
- TCK Madde 329 (Devletin güvenliğine ve siyasal yararlarına ilişkin bilgileri açıklama)
- TCK Madde 330 (Gizli kalması gereken bilgileri açıklama)
- SPK Bilgi, Belge Ve Açıklamaların Elektronik Ortamda İmzalanarak Kamuyu Aydınlatma Platformuna Gönderilmesine İlişkin Esaslar Hakkında Tebliğ

6698 sayılı Kişisel Verilerin Korunması Kanunu

HATALAR

- Anti-virüs yazılımımız var dolayısıyla güvendeyiz.
- Kurumumuz güvenlik duvarı (firewall) kullanıyor dolayısıyla güvendeyiz.
- Bir çok güvenlik saldırısı kurum dışından geliyor!
- Verilerimin kopyasını alıyorum, güvenlikten bana ne!
- Güvenlikten **Bilgi İşlem** sorumludur!
- Bize kim neden saldırsın?

ZARARLI YAZILIMLAR

Virüsler / Wormlar

Bilgisayarlarınıza saldırmak için tasarlanmış, verilerinizi kopyalayan, tahrip eden veya silen yazılımlardır.

Casus yazılımlar

Gizlice çevrim içi hareketlerinizi izleyen, kaydeden veya sonsuz popup reklamları şeklinde davranan yazılımlardır.

Truva atları

Verilerinizi bozarken veya bilgisayarınıza zarar verirken size yardımcı olan programlarmış gibi görünen virüslerdir.

BGA SECURITY

-Teşekkürler-

bgasecurity.com | @bgasecurity