



Mahremiyetinizi Koruyun

Fatih Özavcı

Bilgi Güvenliği Danışmanı

fatih.ozavci@gamasec.net

[@fozavci](https://twitter.com/fozavci)

viproy.com/fozavci

Büyük Birader seni izliyor....

1984, George Orwell

Mahremiyet

- Mahremiyet
 - TDK : Kişisel Gizlilik
- Değişen dünyada, bireyin sahip olduğu hakların ve bilgilerin, daha güçlü olan devlete karşı korunması gerekliliği oluşmuştur.
 - Devletin Kendini Korumak İstemesi
 - Sahip Olmanın Dayanılmaz Hafifliği
 - Demokratik Haklar ↔ Sözde Özgürleştirilmiş Yasalar
 - Sahip Olunan Kritik Bilginin Kimliksiz Biçimde Paylaştırılması

Mahremiyet İhlalleri

➤ Olağan İhlaller

- Siyasi Fişleme
- Polis Devleti
- Korku İmparatorluğu

➤ Terörizmin Etkisi

- Ülkelerin Havalimanı Kurallarının Değişmesi
- İstihbarat İmkanlarının Arttırılması
- Kişisel Mahremiyetin Azaltılmasını Destekleyen Kanunlar
- Gözaltı, Sorgulama ve Ceza Kavramlarının Evrimi

➤ Gezi Parkı Direnişi Etkisi

- Güçlü Bir Etki, Ancak Yıllar Sonra Tam Olarak Anlayabileceğiz

Mahremiyet İhlalleri

➤ Dolaylı İhlaller

- Cep/Sabit Telefon Dinleme
- Cep Telefonundan Yer Saptama
- Kameralarla Sürekli İzleme
- Parmak İzi Temelli Doğrulama
- E-Postaların Takibi
- Facebook/Myspace/Twitter/Instagram İşbirlikleri
- Skype/VoIP Görüşmelerinin Kaydı

➤ Doğrudan İhlaller

- Havalimanında Taşınabilir Bilgisayarın Analizi
- Servis Sağlayıcı Üzerinden İletişimin Kaydedilmesi
- İnternet İçeriğine Erişim Kısıtlaması

Kahrolsun Büyük Birader !

1984, George Orwell

Uyarı !

- Biz ÖZGÜR YAZILIM Öneriyoruz. Güvenilir ve Güvenli !
- Sunum Gereği Maalesef Kapalı Yazılımlar Anılacaktır :(
- Her Konu Farklı Açılardan Anlatılacak ve Örneklenenecektir
 - Masaüstü/Taşınabilir Bilgisayar vs Mobil Cihazlar
 - Android vs iPhone



Güvenli Depolama ve Saklama

Veri Depolama Gizliliği

➤ Veri Depolama Gizlilik Gereksinimi

- Havalimanı Geçişlerinde Taşınabilir Bilgisayar/Disk/Kart
- Olası Gözaltında Kişisel Verilerinizin İfşası
- Taşınabilir Bilgisayar/Disk/Kart'ın Kaybolması veya Çalınması
- Bir Diskin/Kartın Satılması, El Değiştirmesi

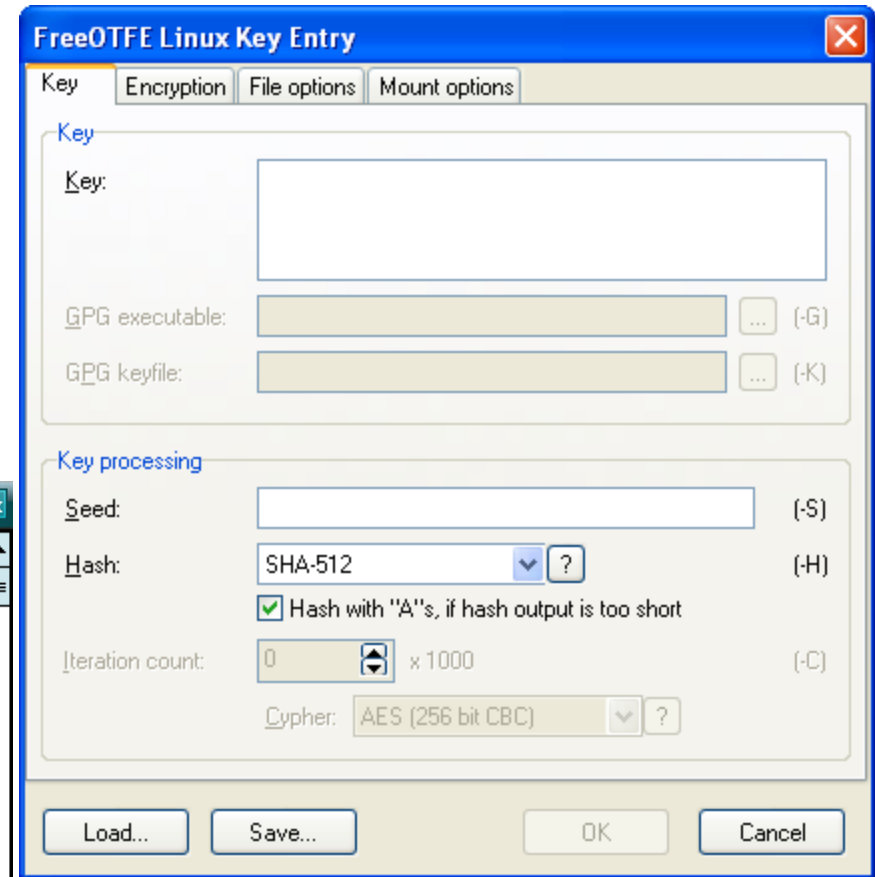
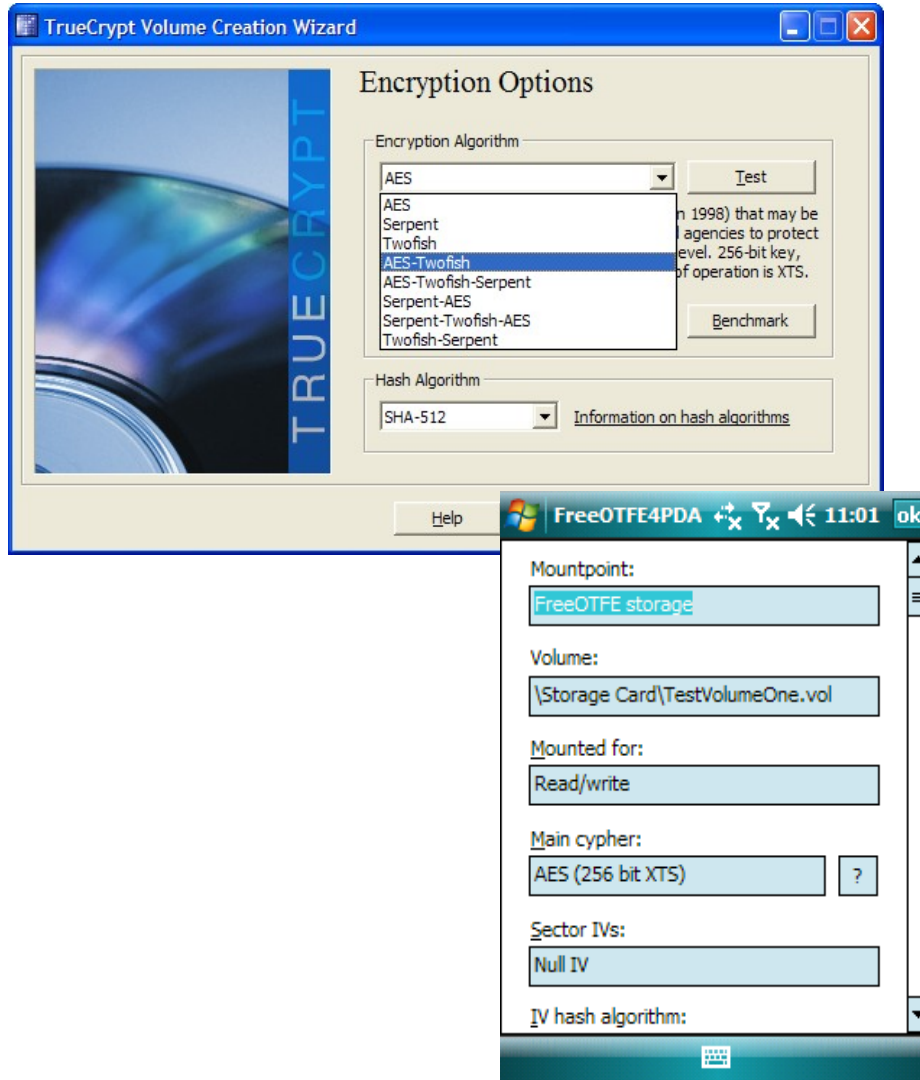
➤ Disk Şifreleme

- Bir Diskin/Kartın Şifrlenmesi
- Özel Bir Dosyanın Kriptolanarak Disk Biçiminde Kullanılması
- Kripto Çözme Anahtarının Saklanması
- Plausible Deniability (Makul Reddedilebilirlik)

Disk Şifreleme Yazılımları

- İşletim Sistemi Çözümleri
 - Mac OS X → Filevault
 - Windows → Bitlocker
 - Linux → Crypto Loopback
- Truecrypt - www.truecrypt.org
 - Sabit Disk, Sanal Bir Disk Dosyası, Kart Şifreleme
 - AES, Serpent, Twofish Algoritma Desteği
 - Windows, Mac, Linux Desteği
 - Şifreleme ve Yasal Nedenlerle Özel Bir Lisans Kullanmaktadır
- FreeOTFE - www.freeotfe.org
 - Sabit Disk, Sanal Bir Disk Dosyası, Kart Şifreleme
 - AES, Serpent, Twofish Algoritma Desteği
 - Windows, Windows Mobile, Mac, Linux Desteği
- Cryptoloop, dm-crypt, LUKS

Ekran Görüntüleri



Adım Adım Güvenli Disk Depolama

- Sabit Diskte Özel Bir Disk Bölümü Oluşturulur
- Disk Bölümü Gizli Bölüm Olarak Atanır
- Disk Bölümü Bir İşletim Sistemi ile İlişkilendirilmez
- Disk Bölümü Biçimlendirilmez (Formatlanmaz)
- Truecrypt ile İlgili Bölüm Kriptolanır ve Depolama Yapılır
- *Harici Hafıza Kartı/USB Belleğe de Uygulanabilir*

Böylece ;

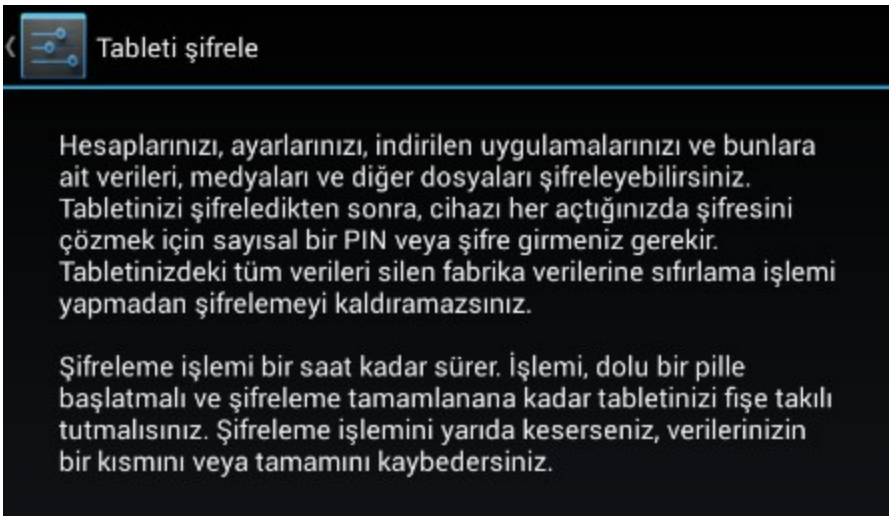
- Şifreleme Çözülmedikçe Veri Anlamlandırılmaz
- Diskin Parçası AMA “Kullanılmayan” Bir Bölüm Görünür
- O Bölümde Depolama Yapıldığı İNKAR Edilir

<http://www.truecrypt.org/docs/plausible-deniability>

Mobil Cihazlarda Disk Şifreleme

- Android ve iOS İşletim Sistemleri Cihaz Şifrelemeyi Destekler
- Her iki İşletim Sistemi de Tam Disk Şifreleme veya Harici Depolamanın Şifrelenmesini Destekler
- Cihaz Kilidi Açıkken Tüm Veri “Zaten” Erişilebilirdir, O Yüzden Gerçekten Tam bir Şifreleme Değildir
- Android ve iOS İşletim Sistemlerine Müdahale Edilmedikçe Çözüm Yoktur
- UNUTMA: Apple Güvenlik Güçleri İsterse Şifrelemeyi Açmaktadır.

http://news.cnet.com/8301-13578_3-57583843-38/apple-deluged-by-police-demands-to-decrypt-iphones/



Taşınabilir Depolama Güvenliği

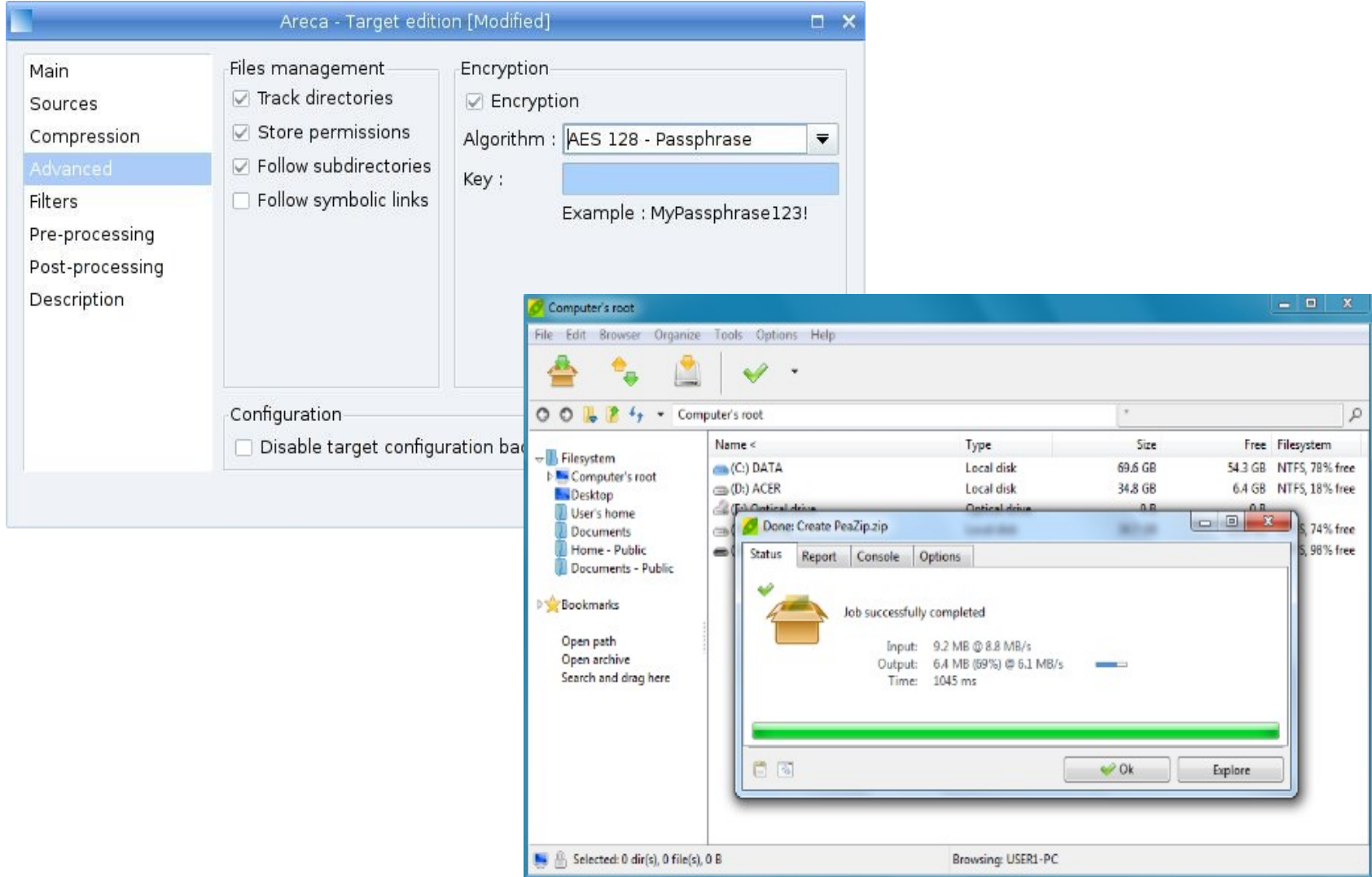
Neden Taşınabilir? Neden Şifreleme?

- E-Posta, Facebook, Twitter “Size Özel Değildir”
- Bir Dosyayı E-Posta ile “Güvenli Biçimde” Göndereceksiniz
- Arşivinizi Kullanmadıkça Kriptolu Depolansın İstiyorsunuz
- Bulut Depolama Kullanıyorsunuz (Dropbox, Google Drive vb)

Ne Kadar Şifreleme? Algoritma? Anahtar İletimi?

- AES-256bit Algoritması Önerilir, Asimetrik Şifreleme “Bilinmiyorsa” Kullanılmamalı
- Arşivi Açacak Anahtar Farklı Bir Yol ile (SMS, Telefon, Kitap) İletilmeli
- Şifreleme Destekli Yedekleme ve Arşivleme
 - Areca – www.areca-backup.org
 - Arşiv (ZIP, ZIP64), AES, Ağ Sürücüsü, FTP/SSL Destekleri
 - Windows, Linux
 - PeaZip – peazip.sourceforge.net
 - Winzip, 7z Uyumlu AES 256 Bit Şifreleme
 - ZIP, DMG, RAR, 7Z, BZIP2 vb.
 - KGB Archiver - kgbarchiver.net
 - AES 256 Bit Desteği

Ekran Görüntüleri

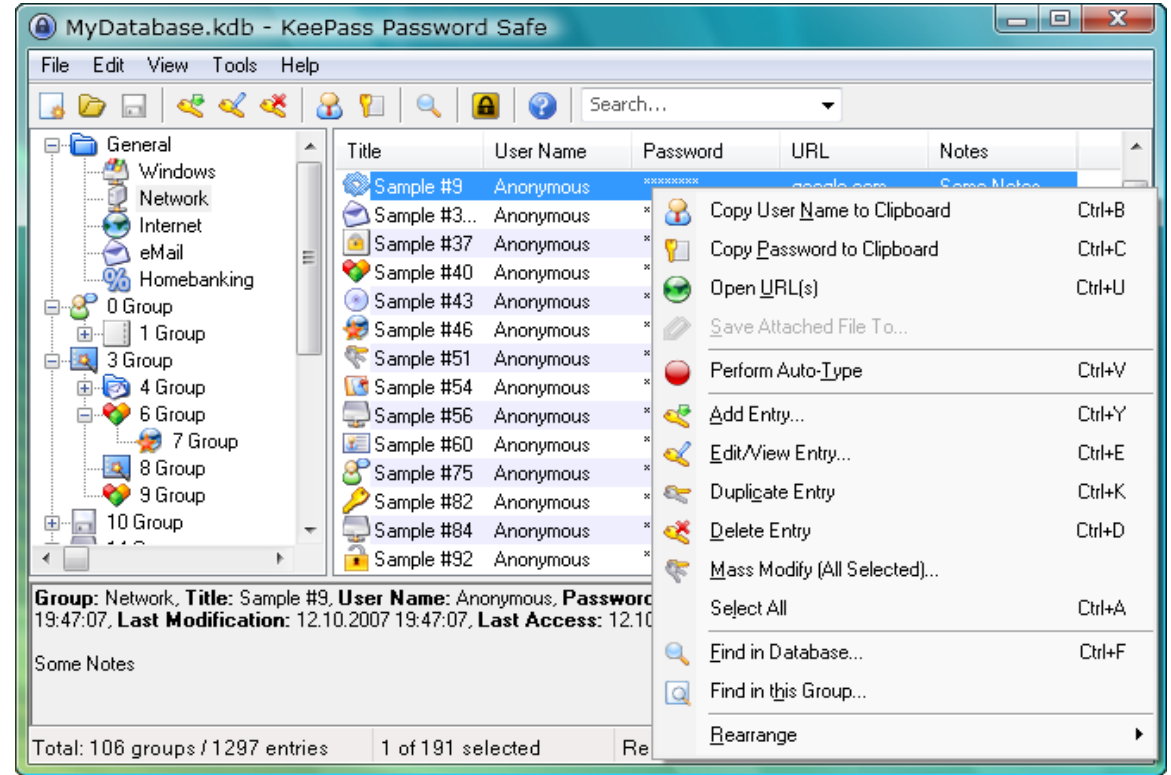


Kişisel Şifrelerin Güvenli Depolanması

- Keepass – keepass.info
 - AES-256 Bit Şifreleme ile Verilen Saklanması
 - Windows, Mac, Linux Desteği
 - Şifre Üretme, Dışarıya Aktarma, Eklenti ve Dil Destekleri

- Password Safe – passwordsafe.sourceforge.net
 - Bruce Schneier Tarafından Geliştirildi
 - Şifre Üretme, Dışarıya Aktarma Destekleri

Ekran Görüntüleri



Güvenli Silme ve Cihaz Sıfırlama

Güvenli Silme

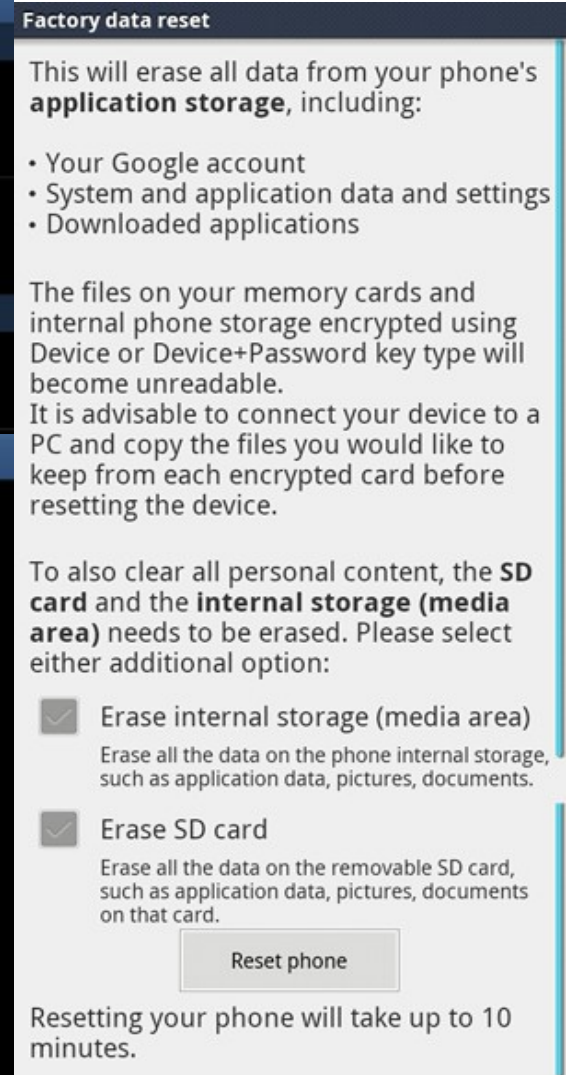
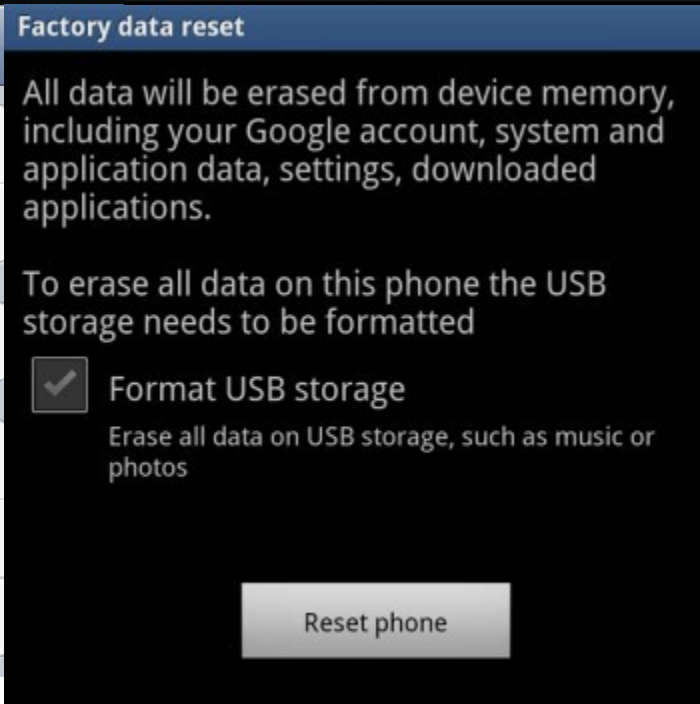
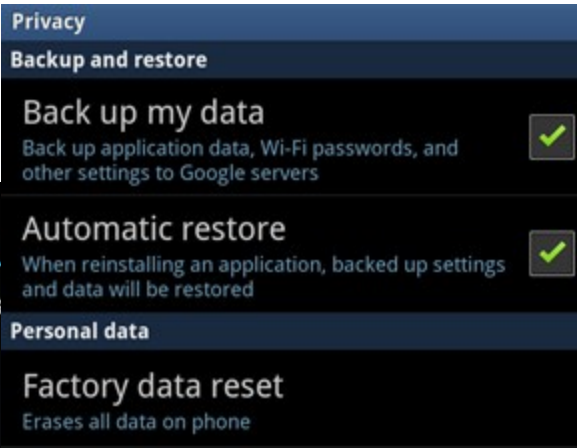
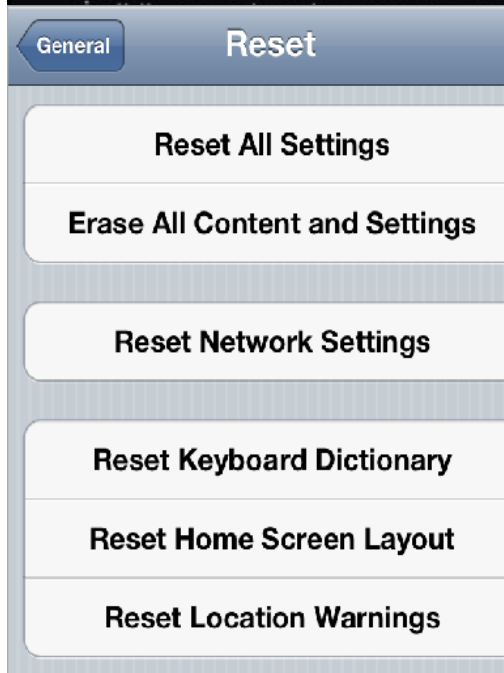
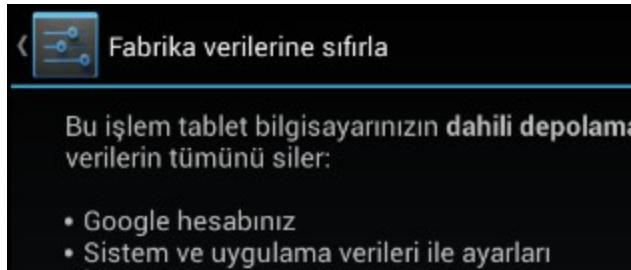
- Dosyayı Sildiniz ama Silindi mi?
 - Çöp Kutusundan da Silmek Yetmez
 - Güvenli Silme Diskteki HAM Veriyi Birçok Farklı Sektöre Taşıyarak Silmedir. Çok Defa Tekrarlanmalı, Her Adımda Üzerine Rastgele Veri Yazılmalıdır
 - Otomatik Yedekleme Yazılımlarına Dikkat (Time Machine, File History)
- Güvenli Silme
 - Wipe – wipe.sourceforge.net / Linux
 - Eraser – eraser.heidi.ie / Windows
 - Mac OS X Dahili Güvenli Silme Desteği
- Mobil Cihazdan Nasıl Sileceğiz?
 - Mobil Cihazlardaki Güvenli Silme Maalesef Çok da Güvenilir Değil
 - Yine de İş Zorlaştırmak Mümkün

Mobil Cihazı Sıfırlama / Silme

- ACİL DURUMDA CİHAZ ile İLİŞKİNİZİ BİTİRİN
- Düzenli Yedek Alın ki Terketmek Kolaylaşsın :-)
- Android Cihazlar Uzaktan Silme Desteğine Sahiptir
<http://support.google.com/a/bin/answer.py?hl=en&answer=173390>
- Çalınan ve KAYBEDİLEN iPhone'u mu Nasıl Bulurum?
Find my iPhone App,
- Cihazı Sıfırlama / Silme
 - iPhone/iPad Cihazları “Sıfırlama” Yapıldığında Güvenli Biçimde Siler. iOS 2.0'dan sonra Güvenli Silme Desteğine Sahiptir
<http://www.ilounge.com/index.php/articles/comments/ios-encryption-and-data-protection/>
 - Android İşletim Sistemi, Kullanılan Sürüme Göre Bağlı Olarak “Güvenli” Silme Desteğine Sahiptir

Android/iOS Cihazı Sıfırlama

Harici Depolama (Micro SD) için önceki adımlardaki Wipe veya Güvenli Silme Yöntemleri



Mobil Cihaz Kullanıcılarına Uyarılar

Mobil Cihazlar Bilgilerimizi Sızdırır!

- Google ile İstatistiklerini Paylaşmak İster misin ?
- Samsung ile Performans İyileştirmeye Ne Dersin ?
- Apple ile Fotoğraflarını Çektiğin Yere Göre Dizer misin?
- Arama Ayarlarını Senin için Özelleştirelim mi?
- Cihazının Bir Yedeğini de Biz Saklayalım mı?
- Kişisel Bilgilerini Bizimle Paylaşmak için 1'e Basar mısın?

- Cevabın “EVET” ise Geçmiş Olsun!

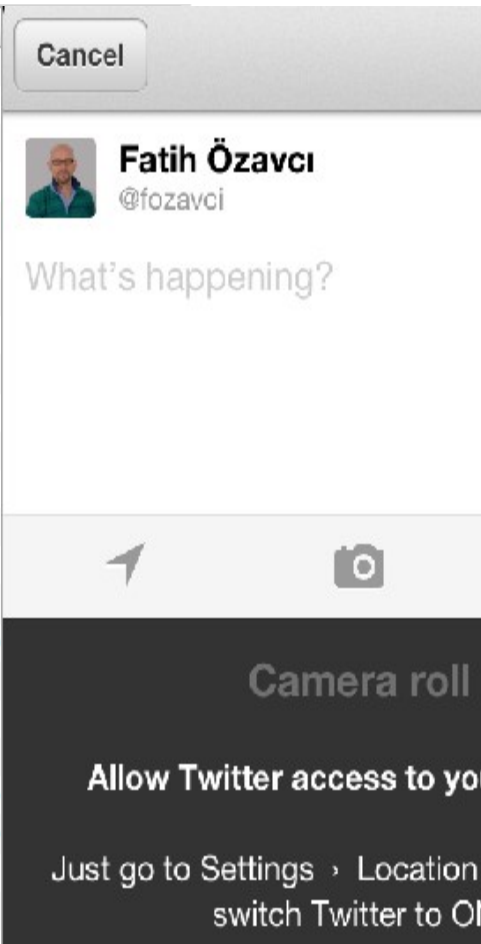
- Mobil Cihazlarda Depolanan Her Veri Cihaz ile İlgili İşaretler ve Bilgiler Taşır.
- Mobil Cihazdaki Bir Fotoğrafı veya Videoyu (İçerik Hassas ise!!!) Temizlemeden Paylaşmayın

Fotoğraflarda Yer Bildirimi

- Fotoğraflarda Yer Bildirimi Destekleyen Platformlar
 - Forsquare, Twitter, Facebook, Instagram, Vine, Whatsapp
- Android ve iOS Siz Yer Bildirimi Seçseniz de Seçmeseniz de Fotoğraflara Çekilen Yerin GPS Verisini Eklemeaktadır
- Kullanılan Android ve iOS Sürümüne Bağlı Olarak, Cihaz ile İlgili Bilgiler de Fotoğraflara Eklenmektedir
- Sosyal Paylaşım Uygulamaları ile Yerleşiminizi “Özel Durumlarda ve Hallerde” Paylaşmayın
- Doğru Dosya Tipi için (JPG, PNG vb.) Doğru Temizleyici
http://en.wikipedia.org/wiki/Comparison_of_metadata_editors
- Mobil Fotoğraf Yazılımınızı Değiştirin
 - Android → “ObscuraCam: The Privacy Camera” vb.
 - IOS → Private Camera Pro vb

Fotoğraflarda Yer Bildirimi

Tag	Value
▼ Camera	
Make	Apple
Model	iPhone 4S
XResolution	72
YResolution	72
ResolutionUnit	Inch
Software	5.1.1
XResolution	72
YResolution	72
ResolutionUnit	Inch
ExifVersion	Exif Version 2.21
ComponentsConfiguration	Y Cb Cr -
FocalLengthIn35mmFilm	35
▼ Image Data	
Orientation	Top-left
DateTime	2013:07:03 13:00
YCbCrPositioning	Centered
Compression	JPEG compression
ISOSpeedRatings	64
DateTimeOriginal	2013:07:03 13:00
DateTimeDigitized	2013:07:03 13:00
PixelXDimension	3264
PixelYDimension	2448
► Image Taking Conditions	
▼ GPS Data	
GPSLatitudeRef	North
GPSLatitude	41° 5.29'
GPSLongitudeRef	East
GPSLongitude	28° 54.23'
GPSAltitudeRef	Sea level



Cihazımda Kilit Var, Açamazlar !

Elbette, Açamazlar...

- Samsung Galaxy S3 / Note 2 Ekran Kilidi Açmak
<http://www.youtube.com/watch?v=6i-0t63wOII&t=87>
- iOS 6.1.3 iPhone Passcode Kilidi Açmak
<http://www.youtube.com/watch?v=QCGJTuTZf8M>
- iOS 7 iPhone Passcode Kilidi Açmak
<http://www.youtube.com/watch?v=wHISiUqomew>
- Çalışan Bir Cihaz Açılırsa Tüm Veriler Erişilebilirdir
- 10 sn.de Terkedemeyeceğiniz Hiç Bir Cihaz Taşımayın
- Cihazınızın Sıfırlama Seçeneklerini Her Zaman Hatırlayın
- Tabi ki Güvenli Bir Yerde Her Zaman Yedeğiniz Olsun

Cihazımı Jailbreak Yaptım, Root'ladım

- Jailbreak işlemi iOS Baseband seviyesinde değişim gerektirir. Güvenlik teknolojilerini kapatır ve kontrol edilmemiş yazılımlar yüklenmesine izin verir.
- “Root”lamak yoktur, Android cihaza “su” veya “sudo” komutunu yüklemek vardır. “Root” sistem yöneticisidir.

Bilinmesi Gerekenler...

- Android Market'te Bile Zararlı Yazılımlar Vardır. İndiren Kişiler, Yorumlar ve Doğrulamaya Bakmadan Yazılım Yüklemeyin
- Android veya iOS Cihazınıza Güvenilmeyen Yazılımları Yüklemeyin
- Ne Yaptığınızı Bilmiyorsanız Jailbreak veya “Root” Hakları ile Erişim Ciddi Güvenlik Sıkıntıları Oluşturur
- Her Zaman Yazılımınızı Güncelleyin. Masaüstü Bilgisayarınız Ne Kadar Hedef ise Telefonunuz da O Kadar HEDEFTİR

HAKARET İÇİN DEĞİL
KENDİNİ KORUMAK İÇİN ANONİM OL!



Anonim Internet Kullanımı

Sizi Kim Takar?

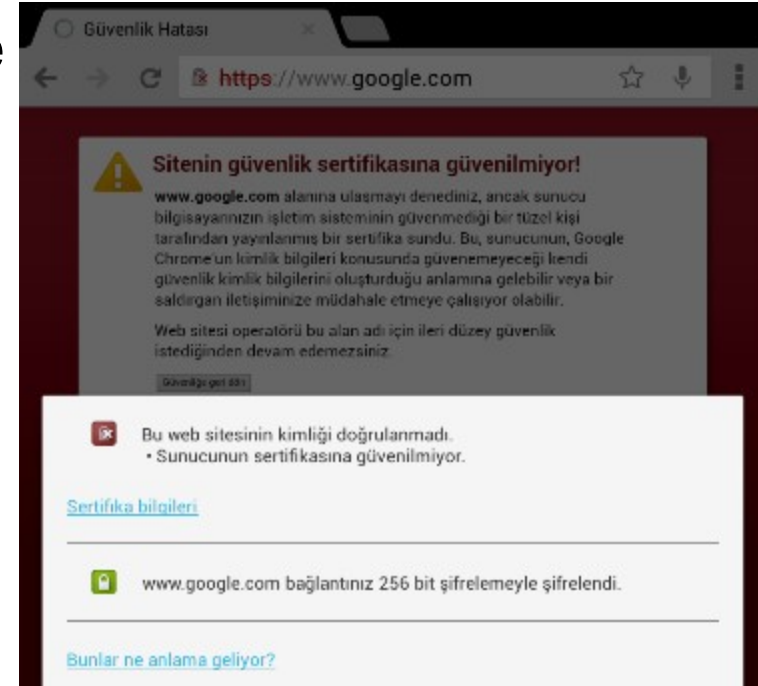
- Kullandığınız Servisler Kişisel Bilgilerinizi Devletler ile Paylaşabilir
- ABD'de Paylaşmaması, Türkiye'de de Paylaşmayacağı Anlamına Gelmez
- Paylaştıklarını veya Hangi Mahrem Bilgilerinizi Verdiklerini Size Söylerler
- Kısaca Internet gibi Kullandığınız Servisler de Güvensiz ve Manipüle Edilebilir

WHO Has Your Back?						
Which companies help protect your data from the government?						
	Requires a warrant for content	Tells users about government data requests	Publishes transparency reports	Publishes law enforcement guidelines	Fights for users' privacy rights in courts	Fights for users' privacy rights in Congress
amazon	★	★	★	★	★	★
Apple	★	★	★	★	★	★
at&t	★	★	★	★	★	★
Comcast	★	★	★	★	★	★
Dropbox	★	★	★	★	★	★
facebook	★	★	★	★	★	★
foursquare	★	★	★	★	★	★
Google	★	★	★	★	★	★
Linked in	★	★	★	★	★	★
Microsoft	★	★	★	★	★	★
myspace	★	★	★	★	★	★
Sonic.net	★	★	★	★	★	★
SPIDERWEB	★	★	★	★	★	★
@twitter	★	★	★	★	★	★
tumblr	★	★	★	★	★	★
verizon	★	★	★	★	★	★
WORDPRESS	★	★	★	★	★	★
YAHOO!	★	★	★	★	★	★

<https://www.eff.org/who-has-your-back-2013>

SSL Güvenli mi?


- SSL İletişimi Uçtan Uca Şifreleme ile Veri Aktarımıdır.
- Sunucunun Sayısal Sertifikası Doğrulanamıyorsa ve Kullanılan Algoritmalar/Protokol Hatalı Seçilmişse Güvenli DEĞİLDİR.
- Sertifika Otoritesine Güvenmek Sertifikaya Güvenmekle Sonuçlanır
- Her SSL Sertifikası Uyarısını Ciddiye Alın, Ortadaki Adam Saldırısı Olabilir
- Ortadaki Adam, Tüm İletişiminizi Dinler ve Kaydeder



SSL Güvenli mi?

- Türk Trust, Sertifika Üretebilecek Bir Alt Otorite Sertifikasını “Yanlışlıkla” EGO ve Bir Başka Şirkete VERDİ.
- İlgili Sertifika 1 Ay Süresince EGO'daki Güvenlik Duvarında Tüm Web Siteleri İçin Ortadaki Adam İşlevi İçin Kullanıldı
- Google Chrome Üzerindeki Sayısal Sertifika Kontrolü ile Sertifikanın Kendi Sertifikası Olmadığını Gördü ve Raporladı

Milliyet.com.tr » Gündem» Haber

05 Ocak 2013 - 02:30 |   A+ A-

Hatalı sertifika devleri alarma geçirdi

Google, Türkiye'nin elektronik sertifika hizmet sağlayıcısı TürkTrust'ın hatalı güvenlik sertifikası verdiğini açıkladı. Ankara taşıma kurumu EGO'nun sitesi, bir ay boyunca güvenli olmamasına rağmen hizmet verdi. Google'ın uyarısıyla


Google, Türktrust'ın 'EGO'suna bozuldu

5 Ocak 2013 |    

 Tavsiye Et 51

 Tweetle 19

 +1 2

 e-posta



ELEKTRİK Gaz Otobüs (EGO) işletmesi başta olmak üzere pek çok Türk kamu kuruluşunun, sahte güvenlik sertifikası kullandığını ortaya çıkaran Google, internet sertifikalandırılması konusunda yetkili kuruluş Türktrust'ı korsanlık yapmakla suçladı. Hatanın muhatabı olan Türktrust ise durum karşısında 'sehven oldu' savunmasını yaptı.

<https://www.turktrust.com.tr/kamuoyu-aciklamasi.1v2.html>

SSL Güvenli mi?

- Devletler ve Devletlerin Sertifika Otoriteleri, Özel Alt Otorite Sertifikalarını Ağ Geçitlerinde Kullanmak Üzere Anlaşabilir
- Güvenli SSL Sertifikası Diye Gördüğünüz Şey, Aslında Bir Başka “Güvenilir” Otorite Tarafından Oluşturulmuş, Gerçek Sertifikanın Bir KLON'u Olabilir
- Çözüm ?
 - Browser'larınızdan Güvenmediğiniz Sertifika Otoritelerini Kaldırabilirsiniz.
 - Silinmelerini Önermediğim Türk Sertifika Otoriteleri
 - Türk Trust
 - Tübitak UEKAE
 - TR-Grid
 - E-Güven
 - KamuSM

İnternette Olmak yada Olmamak

➤ Mahremiyet Sorunları

- Ziyaret Edilen Sayfaların Proxy'lerde, Yazışmaların E-Posta Sunucularında, VoIP Görüşmelerinin Servislerde Kaydedilmesi
- Ziyaret Edilecek Sayfalara Kısıtlama veya Engelleme
- Sadece Belirli Uygulamaların Kullanımına Zorlanma

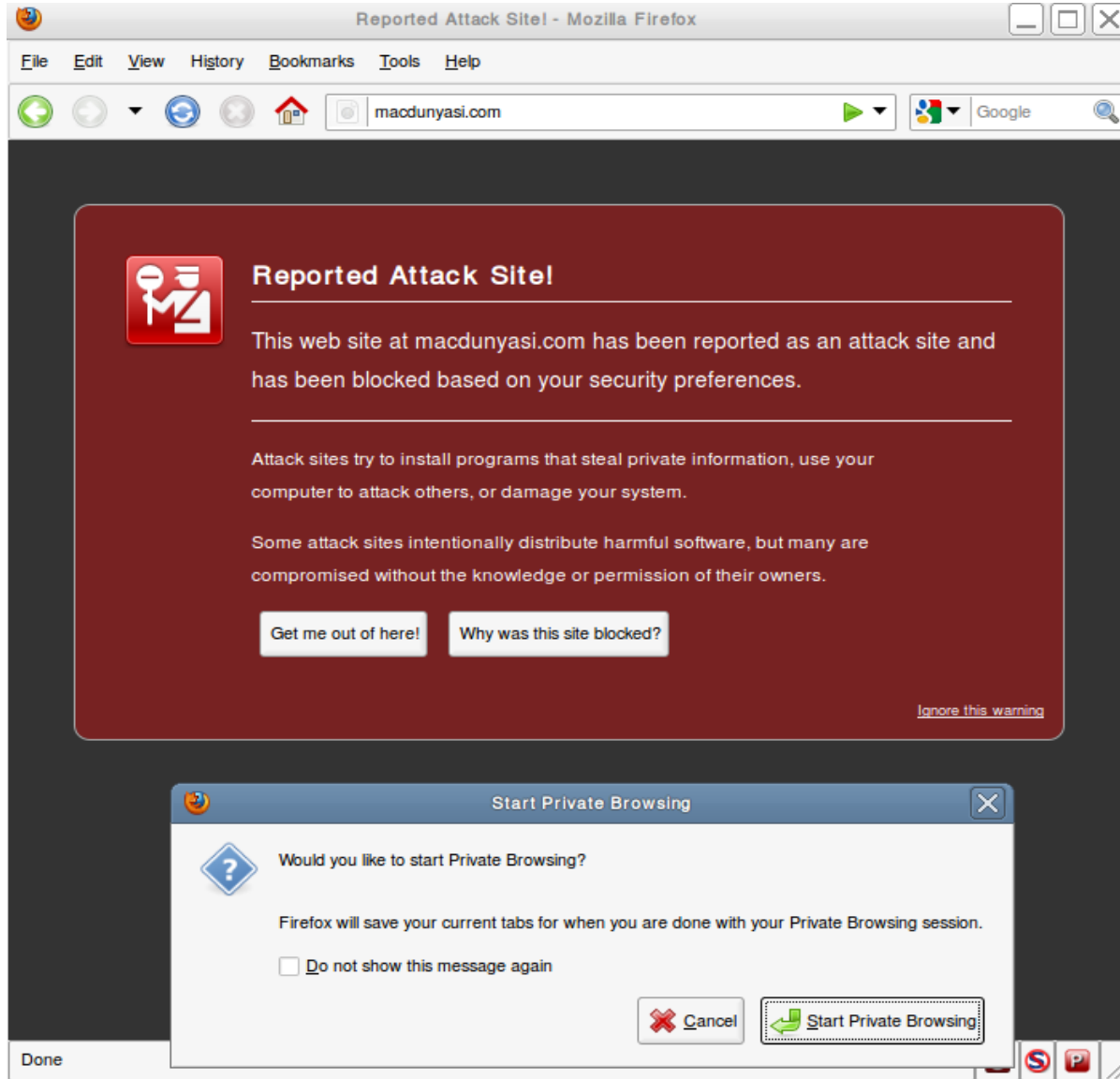
➤ Anonim Proxy Kullanımları

- Tor Projesi – www.torproject.org
 - Dağıtılmış, Anonim Bir Ağ
 - Devlet Kuruluşları İstihbarat Amaçlı, Farklı Ülkelerden Geliyormuş Gibi Kullanmaktalar
 - Tor'da Olan, Tor'da Kalır
 - Windows, Mac, Linux Desteği
 - Harici Proxy'ler ile Desteklenmeyen Uygulamalara Arayüz
- Sınırlandırmaların Aşılması, Takibin Zorlaşması

İnternette Güvenli Gezmek

- Mozilla Firefox – firefox.org
 - Açık Kaynaklı İçi Biliniyor; Kayıt, Kopyalama, İstatistik
 - Geçmiş ve Geçici Depolama Yönetimi İçin Özel Seçenekler
 - Özel Gezme için Ayarlar
 - Eklenti Desteği
 - NoScript
 - Privacy+
 - ViewCookies
 - Ortalama Saldırılarına Koruma
 - Hızlı Güncelleme Yönetimi
- Privoxy – www.privoxy.org
 - Tor için Proxy Desteği

Ekran Görüntüleri



37

Anonim ve Güvenli Haberleşme

Anonim E-Posta ve Sosyal Media Hesabı Sahibi Olmak

- Mutlaka Web Temelli Bir E-Posta Servisi Tercih Edilmeli
- Servisin Ülke Hükümetleriyle Bilgi Paylaşma Politikası İncelenmeli
- Abone Olunurken Hiçbir Özel Bilgi Verilmemeli (Parola Dahil)
- 'İlk Kayıt'tan 'Her Okuma Anı'na Kadar TOR Ağından İletişim Kurulmalı
- Harici Yazılımlar Kullanılıyor ise TOR Ağı Üzerinden Çalıştığı Kontrol Edilmelidir
- Sosyal Ağlara Özel Olarak Alınan E-Posta ile Abone Olunmalıdır

E-Posta Şifrelenmesi

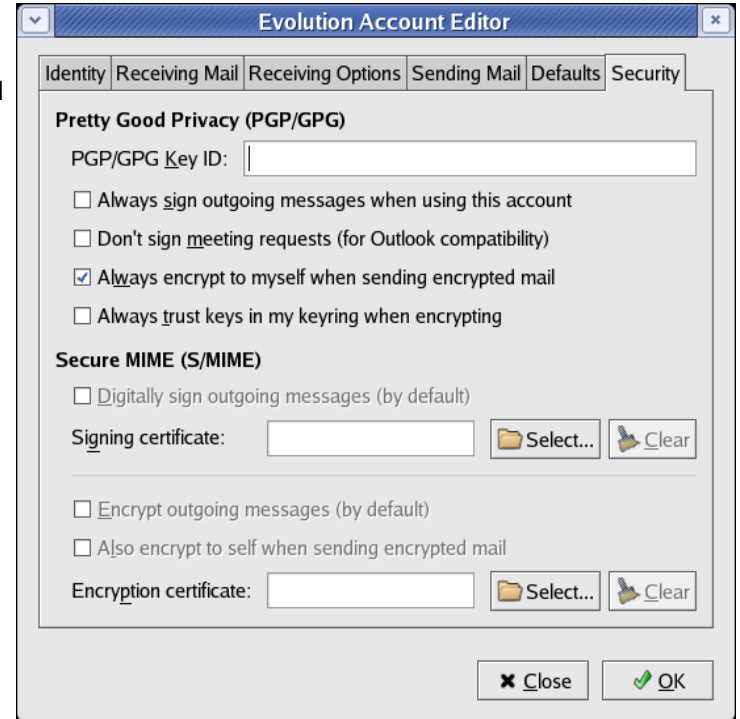
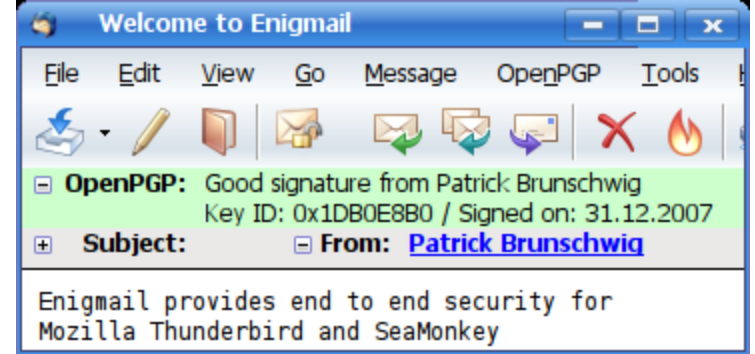
- **Mozilla Thunderbird** - www.mozillamessaging.com/en-US/thunderbird
 - Açık Kaynak, Spam/Ortalama Koruması, Eklenti Desteği
 - E-Posta Resmi Göstermeme, Otomatik Güncelleme, Okuma Bilgisi
- **GPG – gnupg.org**
 - Açık Anahtarlı Şifreleme Altyapısı
 - Simetrik, Asimetrik Şifreleme, Sayısal İmzalama
 - Açık Anahtar Yönetme Sunucuları, Bireysel Güven Yönetimi
 - Windows, Mac, Linux
 - Yaygın E-Posta, Yazışma, Depolama ve İletişim Yazılımlarının 3. Parti Eklentiler/Yazılımlar ile Entegrasyonu
 - GPG Arayüzleri - gnupg.org/related_software/frontends.en.html
- **E-Posta Yazılımları Entegrasyonu**
 - Mozilla Thunderbird, Enigmail
 - Evolution
 - MS Outlook Eklentisi, GPGol, GPGOE

Ekran Görüntüleri

-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.0.4 (GNU/Linux)

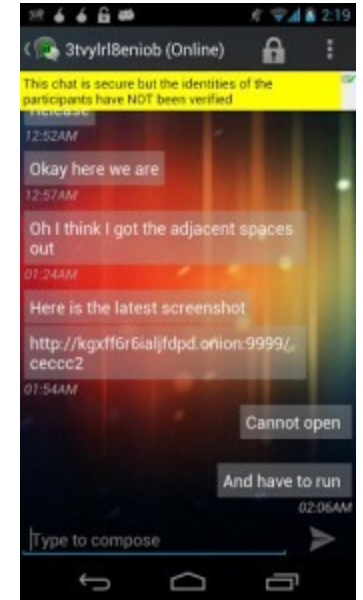
Comment: Gnome PGP version 0.4

hQIOA7HMZGc8Py7SEAf/eWVrPAF/k75uWRthVdsQcy7e725F2cl5kQDIDI44/KdP
vyaCEMd+4eVqEh3Ao3PmdGzAc31KGLA56sWPYySk4f7YlbyRF8bLL1odZNa3Mbwu
B0mH6vsUDmgMAoSSvTn3ckWNaDaVjXMn1RFD+1yzrs/hCoBzTMx12aH628JE+qeg
KG9fRununsabmV3a29uaZKSaxyXIBMvms7E377SEuiDj+Q4+xjqVL49v8u9nWci
EaUovJEcrJVDBEP/575jc6DJZZ9I448nK5IHPv68O8s+xwZ7GESGHfLUcoBPcn
HOuUc7I9o2dry+zFDT9alsWGtPL9nSMJ1fSGNbpbkLQf9Hybi96v8QEp8F+8bomHs
qEfsumlxWRsMtNNj3gc3YAZquiUGDqcUD58uOssUqe/vdE6LaTV99rPTHl2zf3r0
sMe7U9CmvFa6h0YkkAt6hoLdkDKM+IXzVNuyibvsWSOez3fko9BJ+YUOLNvTgWwO
rTIX6c+f2tObTk9P3jzzu9qy2GVgV8zajd23Bh12JTLygBhOa4WivYibVvCNHu3n
DdpgQ9WaSVWSsKyE9wLYxM90Wz3cVjFeNd2ZQslxoxZv+1yTyyIR1nOpz5MjuGrZ
WPLVTJhfUUeAbOsqF2MhIEW0XH+j25DWgUrnK0CxPKC1TR3hX8yHhGPglow+MFH
LNKRAdJ5uOqgd3ET6NfV5x2gFaW2Bn/fta024Z1P4IEQ/dis3M8QW/71Z5CZ7/8w
MUREmJiEaWc6YOxahWO/2D3i5DfIM2dArDRu4c9hXIA5+dwyxewEKerGUvb1X5X0
9ZFgULUtWKXC7ZzoODxvIQvCUBO+nMUD/lo4OAPDxWrHKHE7IDhpCBGxa/ja/9fD
XtwrvA===nDBS
-----END PGP MESSAGE-----



Anlık Haberleşme Güvenliği

- Whatsapp, Facebook, Gtalk Standart Güvenlik Seviyesindedir
- Ek Şifreleme Desteği Olmadan Bir İletişim Güvenli Olamaz
- Gibberbot - <https://guardianproject.info/apps/gibber/>
 - Windows, Linux, Mac, iOS, Android
 - Şifreleme Desteği Bulunmaktadır
 - TOR Desteği Bulunmaktadır
 - Özgür Yazılımdır, Koduna Güvenilebilir



Cep Telefonu Kullanmayacak mıyız?

- Normal Cep Telefonları Operatörleri Ölçeğinde Güvenilirdir
 - Devlet İş Birliği, Yasalar, Bilgi Toplama Zorunlulukları
- Çağrı Dinlenebilir mi? Gönderilen SMS'ler Görülebilir mi?
 - Basit Bir Sahte GSM Noktası ile Baskın Sinyal Yaymak Mümkün
 - 3G → 1G İndirme, Güvenlik Önlemleri Devre Dışı (Femtocell?)
 - Operatör, Devlet Görevlisi veya Art Niyetli Biri Yapılabilir
- Önlem ?
 - Telefonda Açık Bilgi Vermeyin, Anlaşmak için İkinci Bir Kaynak/Bilgiye İhtiyaç Duyulsun
 - SMS Kullanmamaya Çalışın, Gibberbot Kullanın
 - Twitter Parolanızı SMS'le Gönderirseniz İlk Fırsatta Değiştirin
- Kriptolu Telefon/Çağrı?
 - Yasal Olarak Mümkün Değil (bkz. Kripto Yönetmeliği 2010)
 - Şifreli SIP/RTSP İletişimi? (Skype Değil, Hatta Uzak Durun :)

Hedefli veya Hedefsiz Saldırıların
Kurbanı Olmamak !

Hedefli ve Hedefsiz Saldırı Farkı

- Hedefsiz Saldırıda, Sadece Size Değil Binlerce İnsana E-Posta Gider, Twit Gönderilir, Web Sayfası Hazırlanır
- Hedef Gözetken Saldırı ise Size Yöneliktir
 - Alışkanlıklarınıza Uygun Oltalama E-Postası Gönderimi
 - İletişimde Olduğunuz Kişiler Üzerinden “Güvenilir” Paylaşımlar
 - Sahte Hesaplar ile Sizi Kışkırtmak ve Hataya Zorlamak
 - Ziyaret Ettiğiniz Site veya Operatörler Üzerinden Saldırı
- Örnek Senaryolar
 - Arkadaşınız @DrenAbbasaga dan gelen bir bağlantı ?
 - Belediye Başkanınızdan gelen tebrik e-postası
 - Ele geçirilmiş ve zararlı yazılım taşıyan özel web siteleri
 - Sosyal ağlarda ve İnternet'teki tüm kaynaklardaki bilgilerden sizin parola profilinizi çıkarmak
 - Özel hazırlanmış zararlı yazılım ile Anti-Virüs yazılımını atlatmak

Saldırıdan Korunmak

- Internet Güvenilir Değildir, Oradaki İnsanlar da Öyle!
- Her Gelen Paylaşım Tıklamayın, Ziyaret Etmeyin
 - Sahte Hesap Olabilir
 - Arkadaşınızın Hesabı Ele Geçirilmiş Olabilir
 - www.microsoft.com gibi zararlı yazılım taşıyan bir site olabilir
- E-Posta Eklerine Dikkat! Emin Olmadıkça Asla Açmayın!
 - Anti-Virüs'e Güvenmeyin, Kolayca Atlatılabilir
 - EXE, BAT, PS1, CMD, DLL, VBS Uzantılarını Taşıyan Dosyalardan Uzak Durun ve Çalıştırmayın. Dosya Yöneticisinin “Bilinen Uzantıları Gizle” Seçeneğini Kapatın. (KEDİCİK.JPG.EXE)
 - PDF, DOC, XLS Gibi Ofis Belgeleri de Ofis Yazılımlarının Açıkları için Özel Hazırlanmış Olabilir. İki Kere Kontrol Edin.

Saldırıdan Korunmak

- Browser Olarak Firefox Kullanın
 - Tarayıcı Kimliğinizi Özelleştirin (User-Agent) ve Saldırı Hedefi Olma İhtimalinizi Azaltın
 - “Java”yı Kesinlik Devre Dışı Bırakın, Javascript ise “NoScript” Benzeri bir Eklenti ile Kontrol Altında Olsun
 - Flash ve PDF Açıklarından Etkilenmemek İçin Devre Dışı Bırakmayı Düşünün. Gerekliyse Flash ve Java Destekleyen İkinci Bir Browser'ı “Özel Amaçlar” için “Dikkatli” Biçimde Kullanın.
- E-Posta, Haberleşme ve Gizlilik İçeren Her Zaman Ssl Üzerinden İletişim Kurun (<https://www.gmail.com> gibi)
 - Şüpheli Durumda veya Ortak Ağ Kullanımında, Sayısal Sertifikanın Sadece Alan Adını Değil, Otoritesini de Kontrol Edin.
- Cep Telefonu ve Taşınabilir Bilgisayarınızda Kullanmadıkça Kablosuz Ağı Kapatın, Otomatik Dahil Seçeneklerini Devre Dışı Bırakın. Sahte Kablosuz Ağlara Dikkat Edin.

Saldırıdan Korunmak

➤ PAROLA EN ÖNEMLİ VARLIĞINIZDIR

- Her Amaç İçin Farklı Parola Kullanmalısınız
- Sıklıkla Değiştirin
- Büyük Küçük Karakter, Sayı, Özel Karakter ve Boşluk Barındırsın

➤ ÖRNEK GÜVENLİ PAROLALAR

- Twitter ŞifremMuall1!
- Facebook ŞifremMuall1!
- Par0laTwitterOlsun!11bir
- Par0laFacebookOlsun!11bir
- H@sret1msin Gmail!

➤ Yukarıdaki Parolalar Örnektir, Lütfen Kullanmayın

Sosyal Ağ Saldırılarından Korunmak

- İstatistik Veren Site veya Uygulamaları Kullanmayın
 - Kimler Sizi Takip Etmiş? Kimler Bırakmış?
 - Paylaşım Listenizi Görün vb.
 - Parolanızı veya Oturum Bilginizi Alarak Kendi Uygulamasını Yetkilendirir. Sizin Hesabınızı Kendi Adına Yönetir.
- Güvenilmeyen Sayfa veya Uygulamaları Yüklemeysin
 - Uygulamalar Gerekli Olandan Fazla Yetki Talep Edebilir
 - Facebook'ta Çok Sayıda Zararlı Uygulama Paylaşım Yapıyor
 - Twitter Üzerinden Çok Sayıda Sahte Takip Yaşanıyor
- Yukarıda Bahsedilen Genel Saldırıları Sosyal Medya Hesabınızı Kaybetmeniz ile Sonuçlanabilir
- Twitter Hesabınızı Kilitlemek Sizi Korumaz, Arşiv Siteleri ve Retweet ile Zaten Yayılırsınız
- Twitter'ı Kilitlemek #Etiket İçin Yazdıklarınızı Kimsenin Okumaması ile Sonuçlanır. Olayın Etkisi Azalır, Korkmayın ve Paylaşın. Sizi Savunacak Yüzlerce İnsan Bulacaksınız.

Bağlantılar ve Referanslar

- Guardian Project : Secure Mobile Apps and Open-Source for a Better Tomorrow
<https://guardianproject.info>
- Taking your laptop into the US? Be sure to hide all your data first
www.guardian.co.uk/technology/2008/may/15/computing.security
- Osalt - Security & Privacy
www.osalt.com/security-and-privacy
- 40 Open Source Tools for Protecting Your Privacy
www.esecurityplanet.com/features/article.php/3788181/40-Open-Source-Tools-for-Protecting-Your-Privacy.htm
- Plausible Deniability
http://en.wikipedia.org/wiki/Plausible_deniability
<http://www.truecrypt.org/docs/?s=plausible-deniability>

Teşekkürler....