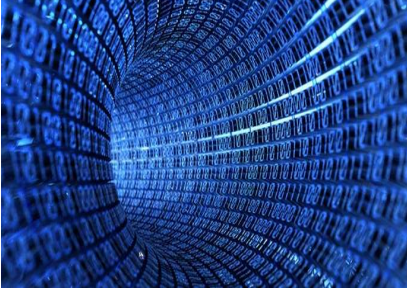


E-GÜVENLİK





Siber Nedir?

Siber terimi sibernetik kökeninden gelmektedir. “İngilizce “**Cyber**” kelimesinden uyarlanıp kullanılmaya başlayan bir **kelime** olup “Bilgisayar ağlarına ait olan”, “İnternete ait olan”, “Sanal Gerçeklik” manalarına gelmektedir.

Siber sadece Internet DEĞİLDİR, çok daha fazlasıdır.

**Ağlar Internet’e bağlı olabildiği gibi olmayabilir de,
(bu bir zorunluluk değildir!)**

Örnekler:

- GPS Uydu Sistemleri, Metro ..vb

Kişisel Veri Siber Güvenlik nedir?



Ağa bağlı sistem ve verilerin yetkisiz kullanım veya zarardan korunması

Bilginin Güvenliđi Nedir ve Neden Gereklidir?

Bilgi güvenliđi, bir varlık türü olarak bilginin **izinsiz** veya **yetkisiz** bir biçimde erişim, kullanım, deđiştirilme, işsa edilme, ortadan kaldırılma, el deđiştirme ve hasar verilmesini önlemek olarak tanımlanır.

Kısaca bir bilginin istenmeyen kişilerin eline geçmemesi ve bizim için bir zafiyet oluşturmaması için gereklidir, önemlidir.

Overview of Cyberwarfare

Siber Savaş nedir

- Siber Savaş nedir?
 - Siber alan çakışması
 - Stuxnet zararlı yazılımı
 - İran'ın nükleer zenginleştirme tesisine zarar vermek üzere tasarlandı
 - Bir PLC için özel geliştirildi
 - İnternete kapalı bir ortama sızıldı



Siber Savaşa Genel Bakış

Siber Savaşın Amacı

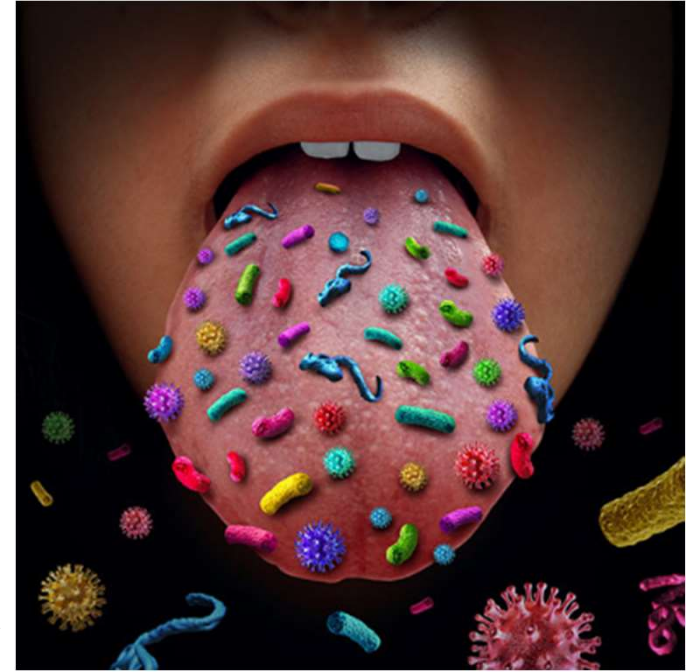
- Düşmanlara, uluslara veya rakiplere göre avantaj elde etmek için kullanılır
 - Diğer ulusların altyapısını sabote edebilir
 - Saldırganlara devlet personeline şantaj yapma olanağı sağlar
 - Vatandaşlara, hükümetin onları koruma yeteneğine olan güvenini kaybettirebilir
 - Hedeflenen ülkeyi fiziksel olarak işgal etmeden vatandaşların hükümetlerine olan inancını etkiler



Kötü Amaçlı Yazılım Türleri ve Belirtileri

Kötü Amaçlı Yazılımın Belirtileri

- CPU kullanımında artış var.
- Bilgisayar hızında bir azalma var.
- Bilgisayar sık sık donuyor veya çöküyor.
- Web'de gezinme hızında bir azalma var.
- Ağ bağlantılarında açıklanamayan sorunlar var.
- Dosyalar değiştirilmiş.
- Dosyalar silinmiş.
- Bilinmeyen dosyalar, programlar veya masaüstü simgeleri var.
- Çalışan bilinmeyen prosesler var.
- Programlar kapanıyor veya kendilerini yeniden yapılandırıyorlar
- E-posta, kullanıcının bilgisi veya rızası olmadan gönderiliyor.



Günümüzde MALWARE trendleri

TTNET

HESAP NUMARASI :
FATURA DÖNEMİ : **Kasım 2014**
SON ÖDEME TARİHİ : **14 Kasım 2014**
ÖDENECEK TUTAR : **251,36 TL**

Rehber Fatura videosu için tıklayınız.

E-Faturamı Görüntüle

URL: <http://efatura.ttnet-fatura.info/goruntuleyebilersiniz>

Faturanızı hesap numarası ile ödeyebilir, otomatik ödeme talimatı ve diğer tüm ödeme işlemlerinizi bu numara üzerinden takip edebilirsiniz.

Kredi kartınızla hemen ödemek veya otomatik ödeme talimatı vermek için [tıklayınız](#) ya da 444 0375 TTNET Müşteri Hizmetlerini arayınız.

Faturanızın arka sayfasını görmek için [tıklayınız](#).

URL: <http://efatura.ttnet-fatura.com/>

Günümüzde MALWARE trendleri

8775563743 nolu hattınıza ait ARALIK-2014 Dönemi Türk Telekom Faturanız

Türk Telekom e-Fatura <haber@eturktelekom.org>

Tarih: 17.12.2014 Çar 15:10

Kime:

TÜRK TELEKOM

E-FATURA (ELEKTRONİK FATURA)



Sayın Müsterimiz,

Son ödeme tarihi **18/12/2014** olan **219,23 TL** tutarındaki güncel faturanıza buradan ulaşabilirsiniz.

[E-FATURA GÖRÜNTÜLE](#)

[E-FATURA ÖDEME](#)

Kağıt tüketimini azaltmak ve çevreyi korumak için e-fatura kullanımı büyük önem taşıyor. Sizde e-fatura tercih ettiğiniz için teşekkür ederiz.

Kişisel Veri

Hedef Olarak Kişisel Veriler

- Neden kimliğini istiyorlar?
 - Uzun vadeli kârlar
 - Tıbbi faydalar
 - Sahte vergi beyannamesi gönderme
 - Kredi Kartı hesapları açma
 - Kredi alma
- Suçlular paranızı nasıl alıyor?
 - Çevrimiçi kimlik bilgileri
 - Hırsızların hesaplarınıza erişmesini sağlar
 - Yaratıcı entrikalar
 - Arkadaşlarınıza veya ailenize para gönderme kandırması



Cihazlarınızı ve Ağınızı Koruma

Bilgi İşlem Cihazlarınızı Koruma

- **Güvenlik Duvarını Açık Tutun**
 - Verilerinize veya bilgi işlem cihazlarınıza yetkisiz erişimi önleyin!
 - Güvenlik duvarını güncel tutun!
- **Anti virüs ve Casus Yazılım Önleme Yazılımları kullanın**
 - Verilerinize veya bilgi işlem cihazlarınıza yetkisiz erişimi önleyin
 - Yalnızca güvenilir web sitelerinden yazılım indirin
 - Yazılımı güncel tutun
- **İşletim Sisteminizi ve Tarayıcınızı Yönetin**
 - Güvenlik ayarlarını orta veya daha yüksek bir düzeye getirin
 - Bilgisayarınızın işletim sistemini ve tarayıcısını güncelleyin
 - En son yazılım yamalarını ve güvenlik güncellemelerini indirin ve yükleyin
- **Tüm Cihazlarınızı Koruyun**
 - Parola koruması
 - Verileri şifreleme
 - Sadece gerekli bilgileri saklayın!



Cihazlarınızı ve Ağınızı Koruma

Kablosuz Ağları Güvenli Bir Şekilde Kullanın!

- Ev Kablosuz Ağı
 - Wi-Fi yönlendiricinizde önceden ayarlanmış SSID ve varsayılan yönetim şifresini değiştirin.
- Herkese açık Wi-Fi noktalarını kullanırken dikkatli olun
 - Hassas bilgilere erişmekten veya göndermekten kaçının
- Kullanmadığınızda Bluetooth'u kapatın
- E-Ticaret yaparken internete ağ üzerinden bağlanmayın.



Cihazlarınızı ve Ağınızı Koruma

Her Çevrimiçi Hesap için Benzersiz Parolalar Kullanın

- Suçluların çalınan kimlik bilgilerini kullanarak tüm çevrimiçi hesaplarınıza erişmesini önler
- Şifreleri hatırlamaya yardımcı olması için şifre yöneticilerini kullanın
- İyi bir şifre seçmek için ipuçları:
 - Sözlük kelimelerini veya adlarını hiçbir dilde kullanmayın
 - Sözlük kelimelerinin ortak yazım hatalarını kullanmayın
 - Bilgisayar adları veya hesap adları kullanmayın
 - Mümkünse ! @ # \$ % ^ & * () gibi özel karakterler kullanın
 - On veya daha fazla karakterden oluşan bir şifre kullanın

OK	Good	Better
allwhitecat	a11whitecat	A11whi7ec@t
Fblogin	1FBLogin	1.FB.L0gin\$
amazonpass	AmazonPa55	Am@z0nPa55
ilikemyschool	ILikeMySchool	!Lik3MySch00l
Hightidenow	HighTideNow	H1gh7id3Now

<http://password-checker.online-domain-tools.com/>

Çok Fazla Bilgi mi Paylaşıyorsunuz?

Sosyal Medyada Çok Fazla Paylaşmayın

- Sosyal medyada mümkün olduğunca az bilgi paylaşın
- Aşağıdaki gibi bilgileri paylaşmayın:
 - Doğum günü
 - E-posta Adresi
 - Telefon Numarası
- Sosyal medya **ayarlarınızı** kontrol edin!



Güvenlik bir ürün değil, bir SÜREÇTİR!

Bruce Schneier

Son Kullanıcılar için Basit Güvenlik Önerileri

- İşletim Sistemi güncellemeleri yapın
- Anti virüs yazılımı kullanın
- Güvenlik Duvarı kullanın
- Lisanssız yazılım kullanmayın
- Düzenli yedek alın
- Güvenli bağlantı kullanın (SSL etc)
- Ekleri dikkatli açın (.zip, .exe dosyalarını açmayın)
- Güçlü şifreler kullanın, kişisel bilgilerinizi gerekmedikçe paylaşmayın