NSA BİZİ İZLEMEK İÇİN GOOGLE REKLAM ÇEREZLERİNİ KULLANIYOR

Kozan Demircan

ABD Ulusal Güvenlik Ajansı NSA ve diğer şirketler ile istihbarat örgütleri kullanıcıları izlemek için Google reklam çerezlerini kullanıyor. Bu çerezler internette gezinmekte kullandığınız browser'a, örneğin Firefox veya Chrome'a eklenerek tarayıcınıza size özel bir tür kimlik numarası atıyor.

Böylece internette bilgisayarınızın IP adresini gizlemek için VPN (Özel Sanal Ağ) ile gezinseniz bile, dikkatli olmazsanız hangi sayfaları gezdiğinizi görebiliyorlar. Reklamverenlerin bize göre özelleştirilmiş online reklam göstermek için kullandığı takip çerezleri aynı zamanda NSA ve diğer örgütlerin web'deki kullanıcı alışkanlıklarımızı görmesini sağlıyor.

Örneğin VPN kullandığınızda IP adresiniz Hollanda'da gözükse dahi, "Bu saatte internete girip Google'da o kelimeyi arayan ve o sayfayı ziyaret eden kişi Ahmet olabilir" diyerek sizi dolaylı yoldan takip edebiliyorlar. Bunun için internete giriş çıkış saatleriniz ile alışkanlıklarınızı analiz eden yazılımlar kullanılıyorlar. Tabii bu bilgileri almak için de çerezlerden yararlanıyorlar. Web'de gezdiğiniz tüm sayfalarda çerez bulunuyor.

İnternette güvenli gezinmek için öncelikle takip çerezlerini (tracking cookies) önlemeniz gerekiyor. Gelin sıradan birer kullanıcı olarak bunu nasıl yapabileceğimizi görelim. Çünkü siz Google sayfasında olmasanız bile Twitter, Facebook gibi sosyal ağlar ve Bing gibi arama motorları hangi sitelere girdiğinizi her an takip ediyor.

NEDEN BİZİ TAKİP EDİYORLAR?

Devletler, istihbarat örgütleri, güvenlik güçleri ve şirketler internette ne yaptığımızı, hangi sayfaları ziyaret ettiğimizi, hangi kelimeler ile neyi aradığımızı takip ediyor. Bunu öncelikle internetten korsan film, müzik, kitap, oyun, yazılım indirip indirmediğimizi anlamak için yapıyorlar.

Web'de teknik takip ile gözetimin ikinci nedeni ise kişisel bilgilerimizi toplayarak kullanıcı alışkanlıklarımızı öğrenmek ve Google'ın yaptığı gibi bize ait bir kullanıcı profili oluşturmak. Böylece bize göre özelleştirilmiş online reklamlar gösteriyorlar. Örneğin, Google'da otomobil kelimesini ararsak veya otomobil sitelerini ziyaret edersek bize otomobil reklamı gösterebilirler.

İnternette teknik takip ve gözetimin üçüncü sebebi, kullanıcı bilgilerimiz ve alışkanlıklarımızı başka şirketlere ya da istihbarat örgütlerine satarak veri simsarlığından (data brokerlığı) para kazanmak. En değerli varlıklarımızdan biri kişisel bilgilerimiz.

Şirketler bunları takip çerezleri ile tarayıcımızdan neredeyse sıfır maliyetle topluyor ve pazar araştırmaları kabilinden üçüncü taraflara, başka şirketlere ya da devletlere satarak büyük paralar kazanıyorlar. Tabii bu süreçte iznimizi almıyorlar veya bize bilgilerimizi sattıkları ya da kullandıkları için para vermiyorlar. Özel hayatımızı, gizliliğimizi ihlal ediyorlar.

*Ah baksana, Bayan Smith'in İngilizce sınıfında 1984 okuyorlar.

MİNAREYİ ÇALAN KILIFINI UYDURUR

Yasal boşluklardan yararlanarak Gmail gibi hizmetlerin kullanıcı sözleşmelerine muallak ifadeler ekliyorlar, örneğin "Bu hizmeti kullanırsan kişisel bilgilerini kullanmamızı da kabul edersin" diyorlar. İnternette bizi gözetlemelerinin son sebebi ise, iktidarların siyasi muhaliflerini fişleyerek sansürleme arzusu. Ancak yazımızın amacı size bütün bu sürecin detaylı analizini yapmak değil.

Yazımızda kısaca sıradan bir kullanıcının internette kişisel gizliliğini nasıl koruyacağını, başkaları tarafından takip edilme şansını önemli ölçüde azaltarak interneti anonim olarak nasıl kullanabileceğini göstermeye çalışacağız.

ÇEREZ CANAVARI

Sözünü edeceğimiz yöntemler gelişmiş teknikler değil ve yüzde yüz koruma sağlamıyor (ki pratikte bu imkansız). Öte yandan, sıradan kullanıcıların internette güvenle gezinmesini önemli ölçüde kolaylaştırıyor. Ayrıca bu yöntemleri kullanmak için uzman olmanıza, kod yazmanıza, bilgisayarınızda karmaşık özel ayarlar yapmanıza gerek yok.

İnternette herkes tarafından takip edilmekten kurtulmak için önce "takip çerezlerinin" ne olduğu ve nasıl çalıştığını açıklamak gerekiyor. İnternet şirketleri kullanıcıların bilgisayarlarına, browser'larına çerez denilen küçük dosyalar yerleştiriyorlar. Çerezler tarayıcılara özel bir takip kodu, bir tür kimlik numarası ekliyor ve online reklam şirketleri ile diğer kişi veya kurumların bizleri internette gözetlemesini sağlıyor.

Firefox gibi bir tarayıcıyı varsayılan ayarlarda, temasını, fontunu değiştirmeden, araç çubuğu eklemeden kullanırsanız daha anonim olursunuz. Tarayıcıyı çok özelleştirmeyin, browser parmak izinizi kolay tespit edemesinler (tabii aşağıdaki gizlilik eklentilerini kurmak hariç).

GMAİL BEDAVA DEĞİL

Google'ın Android tabanlı cihazlar veya internet üzerinden size bedava hizmet verdiğini sanıyorsanız yanılıyorsunuz. İnternet bedava değil: Gmail, Bing, Hotmail gibi hizmetler bedava değil, tersine markette satılan 1 kilo ithal peynirden daha pahalı hizmetler.

Çünkü Google gibi şirketler bunların maliyetini karşılamak için size reklam gösteriyor. Bu reklamları göstermek için de internette ne yaptığınızı takip ediyor. Böylece size göre özelleştirilmiş reklamlar göstererek para kazanıyor.

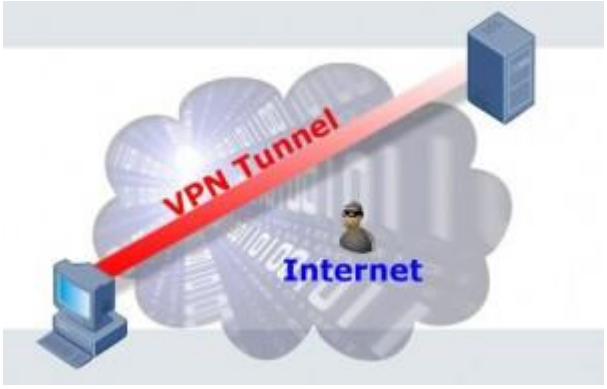
Bu takip çerezlerini engellemek kolay değil. WordPress blog sayfanızdan Twitter ve Facebook'a kadar her yerde takip çerezleri var. Bir arkadaşınızın blogunu beğendiğinizde Google, Facebook ve Twitter'ın bundan haberi oluyor.

DEVLET BABA, ŞİRKET ANA BENİ İZLEMENİZİ İSTEMİYORUM!

Hatırlayacak olursanız bir süre önce tarayıcılara ve bazı sosyal ağlara "beni izlemeni istemiyorum" (do not track me) seçeneği eklendi. Ancak Stanford Üniversitesi İnternet ve Toplum Merkezi'nden Jonathan Mayer bu çabanın geçenlerde sekteye uğradığını söylüyor. Online reklam şirketlerini temsil eden büyük bir ticari grup görüşmelerden çekildi.

Çünkü tarayıcınızda "beni izlemeni istemiyorum" seçeneğini işaretlediğinizde reklamverenler size reklam gösteremeyecekler. Bu da Google gibi arama motorlarıyla sosyal ağların büyük para kaybetmesine yol açacak. Çerezleri kaldırmak şirketlerin işine gelmiyor.

Apple'ın Safari tarayıcısı gibi bazı browser'lar "üçüncü taraf çerezlerini" otomatik olarak engelleyen bir sistem kullanıyor. Mozilla Firefox da bu fikir üzerinde çalışıyor. Ancak, bu ayarlar kullanıcıların Google sayfasını veya Twitter'ı açtığında çerez takibine uğramasını engellemiyor. İşte bu yüzden VPN ve diğer gizlilik çözümlerini bir arada kullanmak gerekiyor.



GÜVENLİ İNTERNET İÇİN VPN KULLANIN

Burada teknik detaylara girmeyeceğiz, ama internette takibi önlemek için yılda yaklaşık 40 dolar ödeyerek yurtdışından hizmet veren bir Özel Sanal Ağ (VPN) hizmeti kullanabilirsiniz. VPN IP adresinizi saklayan bir sistem, kurumsal şirketlerde görmüş olabilirsiniz. İnternete normal bağlandıktan sonra Outlook hesabınıza girer gibi kullanıcı adı şifrenize girerek bir de VPN'e bağlanıyorsunuz.

Diyelim ki internete TTNET'ten bağlanıyorsunuz. Bilgisayara VPN kurduğunuzda internet (ADSL) sinyali TTNET'ten geliyor. VPN girdiğinizde ise, internet bağlantınız VPN şirketinin sağladığı yazılımla şifreleniyor ve IP adresiniz başka bir ülkeden bağlanıyormuşsunuz gibi gözüküyor. Üstelik bu adres başka kullanıcılar tarafından da kullanılan ortak bir anonim adres. Kısacası VPN sizi internet servis sağlayıcınızın gözlerinden saklayan gizli bir tünel.

TTNET'ten baktıklarında IP adresiniz gözükmüyor, internette sizi göremiyorlar. IP adresiniz VPN hizmetine bağlandığınız ülkeye göre değişebilir. Hollanda veya Almanya

olarak gözükebilir. Bunu test etmek için checkmyip.com sitesini ziyaret edebilirsiniz. Siteye girdiğinizde size bilgisayarınızın IP adresini ve bulunduğunuz şehri gösterecek (mesela İstanbul). İşte VPN'den bağlandığınızda bu adres gözükmeyecek. VPN şirketinin sağladığı IP adresi gözükecek, belki İstanbul yerine Seattle.

HANGİ VPN HİZMETİNİ KULLANMALI?

Piyasada BTGuard gibi çok sayıda VPN hizmeti var. Ancak ben Private Internet Access hizmetini kullanmanızı öneriyorum. Öncelikle bu hizmet sunduğu VPN yazılımını yeni teknolojilerle sürekli güncelliyor ve en gelişmiş şifreleme standartlarından bazılarını seçmenizi sağlıyor.

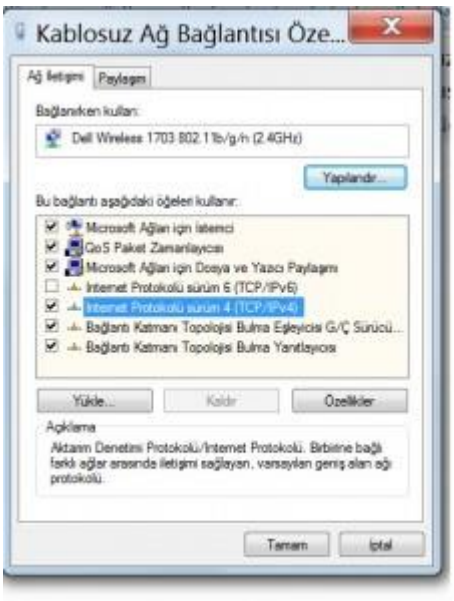
İkinci olarak çoğu VPN hizmeti aslında IP adresinizi saklamayı başaramıyor! Torrent indirirken veya internette gezerken gerçek IP adresiniz bir anda görünür oluyor. Bunun iki yaygın sebebi var. Birincisi DNS leak (DNS sızıntısı), diğeri ise IPv6 internet iletişim protokolü sızıntısı. Bu sızıntıları önleyen ve IP adresini her zaman gizleyen bir VPN hizmeti kullanmalısınız. Açıkçası BTGuard işe yaramıyor. Gerçek IP adresinizi görüyorlar. Bizzat denedim.

Private Internet Access bu hizmeti veriyor. VPN iletişim kutusunda DNS leak ve IPv6 korumasını etkinleştir adlı iki kutu var. Her iki kutuyu da işaretlemeniz gerekiyor. VPN sağlayıcınızın IP adresini gerçekten gizleyip gizlemediğini öğrenmek için http://checkmyip.com/ ve www.checkmytorrentip.com sitesini kullanabilirsiniz.

Torrent indirirken PeerBlock yazılımını kurmanızı da tavsiye ederim. Bu yazılım torrent'te indirdiğiniz yasal içeriğe rağmen hangi videoyu indirdiğinizi takip eden siteleribloklayacak.

Torrent indirmeye başlamadan önce PeerBlock'u çalıştırın. Bu yararlı yazılım film ile müzik sektöründen sizi takip eden, hangi dosyaları indirdiğinizi, kim olduğunu öğrenen adresleri engelliyor ve geliştiriciler tarafından sürekli güncelleniyor.

Not: PeerBlock açıkken Ogame gibi bazı internet siteleri açılmayabilir. Telaşlanmayın. PeerBlock'u kapatıp yeniden deneyin. PeerBlock + VPN + uTorrent güvenli bir yoldur. Burada verilen bilgileri yasal çerçevede kullanmak ve sansürcülere koz vermemek sizin sorumluluğunuzda.



VPN İÇİN SORUN GİDERME

Önce Private Internet Access bağlantısını kesin. sonra VPN arayüzünden çıkın ve ardından bilgisayarınızı kapatın. Bunu yapmazsanız gelecek sefere internete bağlanamayabilirsiniz (sık tekrarlanan bir hata). Bunu çözmek için aşağıdaki yöntemi uygulayın:

Windows 7'de Denetim masası > Ağ paylaşım merkezi > Bağdaştırıcı ayarlarını değiştirinsekmesine gidin. Kullandığınız internet bağlantısının simgesine sağ tıklayın (kablosuz ev bağlantısı, Ev Ağı – İsmail vb.). 'Özellikler'i seçin. Açılan pencerede IPv6yazan kutunun işaretini kaldırın. IPv4 yazan kutuyu seçin. Sağ altta yine 'Özellikler' düğmesini tıklayın.'Otomatik olarak bir IP adresi al' radyo düğmesini seçin. Ayrıca 'DNS sunucu adresini otomatik olarak al' radyo düğmesini seçin. Tamam diyerek kapatın.

İnternete bağlandıktan sonra VPN'i başlatın. Bilgisayarı kapatmadan önce VPN'i düzgün kapatırsanız bu sorunu yaşamazsınız.

DNS SIZINTISINA DİKKAT!

Özellikle torrent indirirken mutlaka www.checkmytorrentip.com sitesine giderek IP adresinizin gizlendiğinden emin olun. IP adresiniz Türkiye değil de Singapur gibi başka bir ülkeden gözüküyorsa sorun yok demektir. Bunun için site size bir test torrent dosyası indirmenizi söyleyecek. Bu zararsız test dosyasını torrent programında (örneğin uTorrent) açıp indirmeye başlarsınız sistem IP adresinizi test edip gösteriyor.

VPN sağlayıcınızın sayfasında hangi IP adreslerinin sağlandığı yazar. Adresleri karşılaştırın. Örneğin BTGuard kullanınca Google DNS ve Open DNS adresleri görünüyor. Buna DNS sızıntısı diyoruz. Bu nedenle torrent indirirken gerçek IP adresiniz de zaman zaman gözüküyor. Private Internet Access'te bu hatayı görmedim. https://www.dnsleaktest.com/ sitesine girerek, VPN'e bağlıyken gözüken DNS adresinin VPN şirketinin kullandığı adres olduğundan emin olun.

Bazı sansürlü siteler VPN'e rağmen açılmıyorsa, DNS sızıntısı nedeniyle gerçek IP adresinizi gören Google DNS gibi DNS sunucularını kullanıyor olabilirsiniz. Ayrıca bu sebeple, torrent indirirken uTorrent gibi bir torrent yazılımı birden gerçek IP adresinizle çalışmaya başlayabilir. Kaliteli hizmet veren bir VPN şirketine abone olmak bu yüzden önemli.

VPN'DE ŞİFRE DE ÇOK ÖNEMLİ

Private Internet Access VPN penceresinde 'Encryption' düğmesini tıklayın. Pencere genişleyecek. Soldan 'Data Encryption'ı AES-256,
'Data Authentication'ı SHA256 ve 'Handshake'i RSA-4096 olarak seçin.

Bu ayarlar size en güvenli şifrelemeyi verecek ve internet hızınızı biraz yavaşlatacak. Varsayılan ayarlar ise standart koruma ve biraz daha hızlı bir internet sağlayacak. Deneyin ve çalışıp çalışmadığına bakın. Sizde çalışmıyorsa, internete bağlanmakta sıkıntı varsa varsayılan ayarlara geri dönün. Elbette VPN şifreniz siz sakladığınız sürece güvenli.

Şifrenizi ve kullanıcı adınızı kimseye söylemeyin, hiçbir yerde paylaşmayın.

Buna ek olarak Private Internet Access hizmetinin bir avantajı daha var. Hizmeti hangi kullanıcının kullandığına dair günlük tutmuyor. Bu hizmeti veren şirket internet açısından riskli bir ülke olan ABD merkezli bir firma, ama günlük tutmadığı için şirkete FBI baskın yapsa bile size ait bilgileri alamaz. Çünkü bu bilgiler VPN sunucularında tutulmuyor.

Peki ya yalan söylüyorlarsa? Aşırı şüpheci olmaya gerek yok. Bu şirket sadece bireylere değil, büyük kuruluşlara da hizmet veriyor ve iş modeli gereği dürüst olmak, sözlerini tutmak zorundalar. Elbette daha güvenli bir internet için ek önemler alabilirsiniz. Bunları başka bir yazıda ele alacağız.

VPN KULLANMANIN ADABI

Öncelikle sıradan bir kullanıcı olduğunuz için hakkınızda özel bir soruşturma olmayacaktır. Yalnızca herkes kadar takip ediliyorsunuz. Bu yüzden güvenli bir VPN şirketi ve aşağıda anlatacağımız birkaç yöntem sizin için yeterli olacaktır.

VPN'e her zaman aynı ülkeden ve aynı saatte bağlanmayın. Farklı ülkeler deneyin, VPN listenizde on kadar ülke var. Rastgele rotasyon yaparsanız NSA ve diğer istihbaratçıların analiz programları internetteki o anonim kullanıcının siz olduğunu anlamakta zorlanırlar.

Twitter'a giriş çıkış saatlerinizin takip edildiğini akılda bulundurun. Twitter ve Facebook'a önceden belirlenen saatlerde, otomatik olarak mesaj atan programlar kullanabilirsiniz. HootSuite gibi bu programların da sosyal medya hesaplarınızı, hatta kullanıcı adı ve

şifrenizi izleyebileceğini unutmayın. Ancak Twitter gibi sosyal ağlara her gün aynı saatte girmezseniz dolaylı takip ihtimalini azaltırsınız.

Herhalde biliyorsunuz, VPN kullanarak Google veya Facebook'a girerseniz gizli kalamazsınız :). Sonuç olarak bu hizmetlere kendi kullanıcı hesabınızla giriyorsunuz. Ayrıca Google'ın arama sorgularınız, aradığınız kelimelerle ilgili daha akalı sonuçlar göstermesi için sizi izlemesi şart. Aynı şey Facebook için de geçerli. Üstelik VPN ile bu hizmetlere girdiğinizde sizin hangi VPN şirketinden hizmet aldığınızı ve hangi ülkeden bağlandığınızı da öğrenecekler. Olsun. Bunda bir zarar yok, güvenli gezinmenin başka yolları da var.

ANONİM ARAMA MOTORLARI KULLANIN

Ixquick arama motoru internette Google'da olduğu gibi arama yapmanızı sağlıyor. Üstelik anonim bir arama motoru, çerez kullanmıyor ve arama verilerinizi takip etmiyor veya kaydetmiyor. VPN kullanırken bu arama motorunu kullanırsanız internette gizli arama yapmış olursunuz.

Aynı şirketin bir de Startpage sitesi var. Bu site de kullanıcı adınızı kullanmadan Google'da sizin adınıza anonim arama yapıyor ve Google sonuçlarını gösteriyor. Startpage anonim Google sonuçlarını kullandığı için, Ixquick'ten daha alakalı ve çeşitli arama sonuçları sağlıyor. Ixquick ise Google'dan tümüyle uzak durduğu için potansiyel olarak daha güvenli, ama daha sınırlı bir arama hizmeti sunuyor (Ixquick kendi arama motorunu kullanıyor, daha az sayıda alakalı sonuç gösteriyor).

MECBUR OLMADIKÇA GİZLENMEYİN

Sosyal medya kullanıyorsanız, sosyal medya uzmanı iseniz; sosyal medya, halkla ilişkiler, pazarlama gibi bir sektörde çalışıyorsunuz internette sürekli gizlenmek işinize gelmez. Google'ın ve sosyal ağların ilgi alanlarınızı, alışkanlıklarınızı bilmesi bu sitelerin size daha

alakalı sonuçlar göstermelerini sağlayacak ve kafa yapınıza uygun Twitter takipçilerini bulmanızı kolaylaştıracaktır.

Ve elbette kendi blogunuzdaki çerezleri önlemek istemezsiniz! WordPress Jetpack, Platinum SEO gibi uygulamalarla sayfanızı günde, haftada, ayda kaç kişinin (tekil kullanıcı) ziyaret ettiğini görebilir, Google arama sonuçlarında sitenizin üst sıralarda (herkesten önce) gösterilmesi için gerekli ayarları yapabilirsiniz.

Örneğin ben işte çalışırken veya yazı yazarken Google arama motorunu kullanıyorum. Twitter çerezlerini filan engellemiyorum, VPN'im her zaman açık ama özelim olursa Ixquick vb. kullanırım. Bu arada güvenli internet için birkaç ipucu daha verelim:

BROWSER'DA ARAMA YAPARKEN DİKKATLİ OLUN

Ixquick ve Startpage arama motorlarını browser'ın tarama kutularına ekleyebilirsiniz (Mozilla Firefox ve diğer tarayıcıların arama kutuları). Bunun için ilgili sitelere girip tarayıcıya arama kutusu ekle düğmesine basmanız yeterli: HTTPS destekli arama kutusu ekleyin, http eklemeyin. Böylece bir arama sonucunu tıkladığınızda önce HTTPS standardında şifre destekli bir sayfaya ulaşırsınız (tabii sitede HTTPS kullanılıyorsa).

Tarayıcınızın arama çubuğundan arama yapmayın. Bu nokta önemli: Her zaman browser'daki arama kutusunu kullanın ve doğru arama kutusunu seçtiğinizden emin olun. Tarayıcınızda TTNET Akıllı Çubuk ve AVG Security toolbar, Yahoo araç çubuğu gibi ek araç çubukları kullanmayın. Bunlar browser'ın adres çubuğundaki aramaları kendi hesaplarına aktarabilirler (örneğin varsayılan olarak AVG veya Yahoo arama kullanabilirler).

HANGİ TARAYICI? HANGİ EKLENTİ?

Maksimum anonim ve gizlilik için TOR browser'ı öneririm. TOR tarayıcısı Firefox'u temel alıyor, ama TOR tarayıcısında çerez takibine izin veren bütün özellikleri kaldırıp kırparak browser'ı kuşa çevirmişler.

Ayrıca TOR yazılımı, Firefox'taki bir güvenlik açığını önlemek için Noscript eklentisiyle birlikte geliyor. Bir süre önce NSA bazı TOR kullanıcılarının kimliklerini bu açık sayesinde ele geçirmişti. NSA şirketler veya personelle işbirliği yaparak yazılımlara bilerek güvenlik açığı ekliyor.

TOR Browser'ı ayarlarını değiştirmeden, eklentileri kaldırmadan ve hiçbir yeni eklenti kurmadan kullanırsınız daha güvenli olur. Burada şunu da eklemek lazım, TOR anonimlik sağlıyor ama güvenlik istiyorsanız VPN kullanmalısınız. VPN + TOR en güvenlisi ancak bunda da dikkat etmek gereken bir nokta var:

TOR maksimum gizlilik sağlamak için browser'da flash video oynatmanıza bile izin vermiyor. TOR ile hemen hemen hiçbir web sitesi çalışmıyor. İşte çalışmak veya internette sıradan bir kullanıcı olarak gezinmek istiyorsanız bunu TOR'la yapamazsınız.

Ancak, Firefox ile yapabilirsiniz. Eklenti zenginliği ve diğer özellikler açısından Firefox en güvenli standart browser olarak biliniyor, ama birkaç küçük ayarla Firefox'u biraz daha güvenli yapabilirsiniz.

Firefox'ta 'Seçenekler'den 'Gelişmiş' sekmesine geçin ve 'Veri Tercihleri' altında Telemetry, Firefox Sağlık Raporu, Çökme Habercisi kutularının

seçimlerini kaldırın. Böylece tarayıcınız Mozilla'ya hata ve çökme verileri göndermeyecektir. 'Seçenekler' 'Gizlilik' sekmesi altında 'Sitelere izlenmek istemediğimi söyle' radyo düğmesini işaretleyin. Böylece takip çerezlerini önlemek için temel korumayı etkinleştirmiş olacaksınız.

FİREFOX TEK BAŞINA YETMEZ

TTNET, gezinti.com sitesi üzerinden Phorm şirketinin sağladığı bir çerez takip sistemini kullanıyor. Böylece internette sizi takip edebiliyor (kullanıcı alışkanlıklarınızı biliyorlarsa VPN'e rağmen sizi izleyebilirler). Konuyla ilgili ek bilgi için enphormasyon.org sitesini ziyaret edebilirsiniz.

Phorm çerezlerini önlemek kolay değil. Phorm çerezlerini önlemek için Özgür Turanlı'nın Phorm Belasından Nasıl Kurtuluruz? sayfasını ziyaret edebilirsiniz. Bu sayfadaki önlemleri almanızı önemle tavsiye ediyorum:

LİNK : http://ozgurturanli.com/google-chrome-kullanicilari-phorm-belasindan-nasil-kurtulabilir/

Yukarıdaki talimatları Firefox'taki benzer çerez ayarlarını bularak uygulayabilir ya da şu siteyi ziyaret ederek Firefox tarayıcınıza Dephormasyon eklentisini kurabilirsiniz (sürekli güncellenen bu eklenti Phorm takibini önleyecek):

LİNK : https://www.dephormation.org.uk

Windows işletim sisteminde Firefox tarayıcı kullanmanızı öneririm. Bu linklerin filtrelenmiş, sansürlenmiş, erişime engellenmiş olması ihtimaline karşı önce VPN'e girebilir ve sayfaları sonra açmayı deneyebilirsiniz.

Dephormation eklentisi Phorm kullanan sitelerden gelen çerezleri engelliyor, fakat Bu sitelere girdiğimde beni uyar seçeneklerini de etkinleştirirseniz internette kimin Phorm şirketi ile işbirliği yaptığını da görmüş olursunuz. Eh hep onlar mı sizi gözleyecek? Biraz da siz onları gözetleyin.

Elbette vatandaşı Phorma'a karşı uyaran bir site Phorm sitesinin adresini veriyorsa Dephormation yanlış alarm verir, endişelenmeyin.

GÜVENLİ İNTERNET İÇİN DİĞER FİREFOX EKLENTİLERİ

Belki web sayfalarındaki reklamları önleyen AdBlock Plus eklentisini duymuşsunuzdur. Ancak ben bu eklentiyi değil, onu temel alan AdBlock Edge eklentisini kurmanızı öneriyorum. AdBlock Edge "Kabul edilebilir reklamlar" seçeneğini kullanmadığı için web sitelerindeki rahatsız edici online reklamları önlemekte daha başarılı. Ayrıca, bazı takip çerezleri veya kodlar online reklamlara da yerleştirildiği için AdBlock Edge eklentisi casus yazılımlardan korunmanızı kolaylaştırıyor.

İkinci kurmanız gereken eklenti Disconnect: Disconnect takip çerezlerini engelliyor. Bunlara Google ve Twitter ile diğer sosyal ağlar da dahil. Böylece Google gibi arama motorları veya Twitter gibi sosyal ağlar hangi blog sayfalarına gittiğinizi, hangi sitelere girdiğinizi göremiyorlar.

Tabii bunlar çalıştığı sürece sevdiğiniz bir blogdaki yazıyı da "like düğmesi" ile beğenemeyeceksiniz. Ancak, Disconnect istediğiniz siteleri beyaz listeye almanızı sağlıyor. Örneğin kendi sitenizi, Facebook, Google sayfanızı veya sevdiğiniz diğer blog sitelerini beyaz listeye ekleyebilirsiniz.

DİSCONNECT

Disconnect gibi eklentiler sizi izleyen görünmez web sitelerini engelliyor. Bu siteleri girdiğiniz sayfada göremezsiniz; ama Firefox menü çubuğundaki Disconnet düğmesini tıklayarak eklentinin işlem penceresini açarsanız, çok sayıda takip sitesinin sizi izlediğini göreceksiniz.

Bu siteler bilgilerinizi reklamverenlere ve arama motorlarına satıyor. Bunlara casus yazılım aracıları da diyebilirsiniz. İşin doğası gereği adlarını saklıyorlar, müşterileri dışında bu sitelerin adlarını sıradan kullanıcı bilmez, yani bugüne kadar bilemezdi. Oysa bugün Disconnect ile sizi kimin gözlediğini görebilirsiniz.

Disconnect çerezleri engelleyince web siteleri daha hızlı açılıyor, "internet daha hızlı çalışıyor", bant genişliğinden tasarruf ediyorsunuz ve kotanız varsa daha yavaş doluyor. Disconnect'in Google'da anonim arama yapmanızı sağlayan çözümleri de var.

DoNotTrackMe: Bu eklenti adından da anlaşıldığı gibi takip çerezlerini önlüyor. Firefox'ta Disconnect'le birlikte kullanabilirsiniz. Aynı işi görüyor ve daha basit bir eklenti. Disconnect gibi sizi gözetleyen siteleri gösteriyor.

MASKME İLE ŞİFRE HIRSIZLIĞINI VE SPAM E-MAİLLERİNİ ÖNLEYİN

MaskMe internet güvenliğinde çok faydalı bir eklenti. Bu eklenti yeni bir sitenin login kutusunda paravan bir e-posta adresi kullanarak gerçek e-posta adresinizi saklıyor. Eklentiyi kurup asıl e-posta adresinizi giriyorsunuz. Ardından bir forumdaki linkleri görmek için o foruma üye olduğunuzda MaskMe sizin için paravan bir e-posta adresi

giriyor, hatta size özel şifre oluşturuyor. Böylece güvenilmez bir siteye ihtiyaçtan dolayı giriş yapmak için gerçek şifrenizi ve e-posta adresinizi kullanmak zorunda kalmıyorsunuz.

MaskMe eklentisi bu yöntemle e-postanızı, şifrenizi, kredi kartı numaranızı, hatta telefon numaranızı saklıyor (son ikisi ücretli sürüm). Özellikle şifre meselesi önemli: Binlerce şifreyi akılda tutamadığımız için, yeni bir siteye üye olurken genellikle e-posta veya Twitter şifremizi kullanıyoruz. Oysa bu şifreyi güvenilmez bir forumdaki geçici üyelikte kullansak, e-posta adresimizi ve Twitter hesabımızı da tehlikeye atmış oluruz. MaskMe ile bu riski önlüyoruz.

Örneğin Financial Times web sitesi siz üye olmadan haberleri okumanıza izin vermiyor. Bu tür sitelere paravan kullanıcı adı ve şifreyle üye olabilirsiniz. MaskMe gerçek e-posta adresinizi bildiği için paravan e-posta adresine gelen tüm iletileri otomatik olarak gelen kutunuza yönlendiriyor. Üstelik spam geliyorsa, spam iletisine Bu adresi otomatik olarak engelle linki de ekliyor.

NOSCRİPT İLE JAVASCRİPT'İ TÜMÜYLE ENGELLEYİN

NoScript tüm Firefox eklentileri içinde en önemli, güvenli ve faydalı eklentilerden biri. Öyle ki TOR Browser'ın son sürümlerinde hazır geliyor! Bu eklenti web sayfalarındaki bütün Javascript kodlarını otomatik olarak engelliyor.

Böylece virüs ve casus yazılım dolu bir siteye girseniz bile bilgisayarınıza kötü amaçlı, zararlı yazılım bulaşma riski büyük ölçüde azalıyor. Tabii Javascript'in engellenmesi Google ve Facebook kodlarının çalışmasını da önlüyor. Kısacası web siteleriniz neredeyse düz sayfa açılıyor. Menüler, düğmeler, videolar, açılır pencereler genellikle çalışmıyor.

PEKİ BU NE İŞE YARAYACAK?

NoScript'in bir sağ tıklama menüsü var. İstediğiniz web sayfasında bu menüyü kullanarak dilediğiniz Javascript satırını çalıştırabilirsiniz. Örnek için yukarıdaki resme bakabilirsiniz: Web sitesindeki hiçbir kod çalışmadığı için siteler size Javascript'i tamamen etkinleştirin diyecek. Buna kanmayın ve sadece istediğiniz komutu etkinleştirin.

Ayrıca sitelere geçici izin vermenizi tavsiye ederim. Böylece izinler tarayıcınızı kapatana kadar geçerli kalır. Bunu yapmazsanız günde onlarca siteye girdiğiniz için hangi siteye kalıcı izin verdiğinizi unutursunuz ve bir sürü siteye izin vermiş olursunuz.

Buradaki espri NoScript'i doğru kullanmak için el alışkanlığı edinmek: Sitedeki Google Analytics'e izin vermezsiniz, ama sitenin kendisine izin verebilirsiniz (torprojectorg'a izin ver gibi). Bir sitede sadece video izleyecekseniz, yalnızca video komut satırına ya da sitenin adına izin verebilirsiniz. Genellikle videolar başka bir siteden çekildiğinden flash videoyu yükleyecek siteye de izin vermeniz gerekecektir.

Özünde basit bir Windows masaüstü sağ tıklama menüsü bu. Yandaki resimde yer alan menüde engelleyebileceğiniz veya geçici ya da kalıcı olarak izin verebileceğiniz komutları içeren sağ tıklama menüsünü görebilirsiniz. Eklentinin web sitesini ziyaret ederek ayrıntıları okumanızı öneririm, meraklı IT'ci arkadaşların bayılacağı detaylar var:

LİNK : http://noscript.net/

AKILLI TELEFONLARDA VPN KULLANABİLİRSİNİZ

Buradaki önlemler akıllı telefonlar ve tabletler için de aynen geçerli. Nitekim Private Internet Access VPN hizmetini mobil cihazlarda da kullanabilirsiniz. Telefonunuza VPN kurabilir ve Firefox tarayıcısı ile bazı eklentiler yükleyebilirsiniz ama bunlar mobil cihazlarda gizlilik için yetersiz kalacaktır:

Android cihazlar ve iPhone'larda kullanılan iOS yazılımı ile diğer uygulamalar, çok daha başka yollardan konumunuzu ve internet bilgilerinizi sürekli yabancılarla paylaşıyor. Doğrusu telefonların IMEI numarasıyla takip edilmesi bile tüylerimi diken diken ediyor. Polisin kaç kayıp telefonu IMEI sayesinde bulduğunu bilmiyorum ama bu numaralarla bizi yakından takip edebileceklerini biliyorum.

Günümüzde mobil cihazlar bilgisayarlar kadar güvenli değil ve güvenlik eklentileri açısından çok daha sınırlı. İnternet güvenle ve anonim olarak gezinmek istiyorsanız bunu PC'den, notebook'tan yapmanız gerekiyor.

Bu yazıda sıradan bir kullanıcının internette rahatça gezinirken makul koruma sağlaması için gereken bilgilere değindik. Elbette kişisel bilgilerimizin gizliliğini korumak için daha güvenli yöntemler de var. Ancak bunları kullanmak için daha ayrıntılı bilgiler gerekiyor. Yazının ikinci bölümünde bu detaylı bilgi sağlayacağım.

```
[status draft]
[nogallery]
[geotag on]
[publicize off|twitter|facebook]
[category istihbarat]
[tags TEKNİK TAKİP DOSYASI, KOZAN DEMİRCAN, NSA, GOOGLE, REKLAM, ÇEREZ]
```