İFADE ÖZGÜRLÜĞÜ KULLANIMINDA HUKUKA AYKIRI TEKNOLOJİK MÜDAHALELERDEN KAÇINMA REHBERİ

TÜRKÇE BASKI



privacyinternational.org

Günümüz teknolojisiyle ifade özgürlüğünü kullanma biçimlerinin de geliştiği, ifade özgürlüğünün daha da güçlendiği düşünülse de dışarıdan müdahalelere daha açık hale geldiği görülüyor. Bu müdahalelerin hukuki-cezai boyutunun yanı sıra, kişisel verilerin kötü niyetli kişilerce ele geçirilmesi olasılığı da vardır. Bu gibi tehlikeler ifade özgürlüğünün etkili bir biçimde kullanılmasının önüne geçtiği ve kişilerin tehlikelerden sakınmak maksadıyla kendi kendilerine otosansür uyguladığı da görülmektedir.

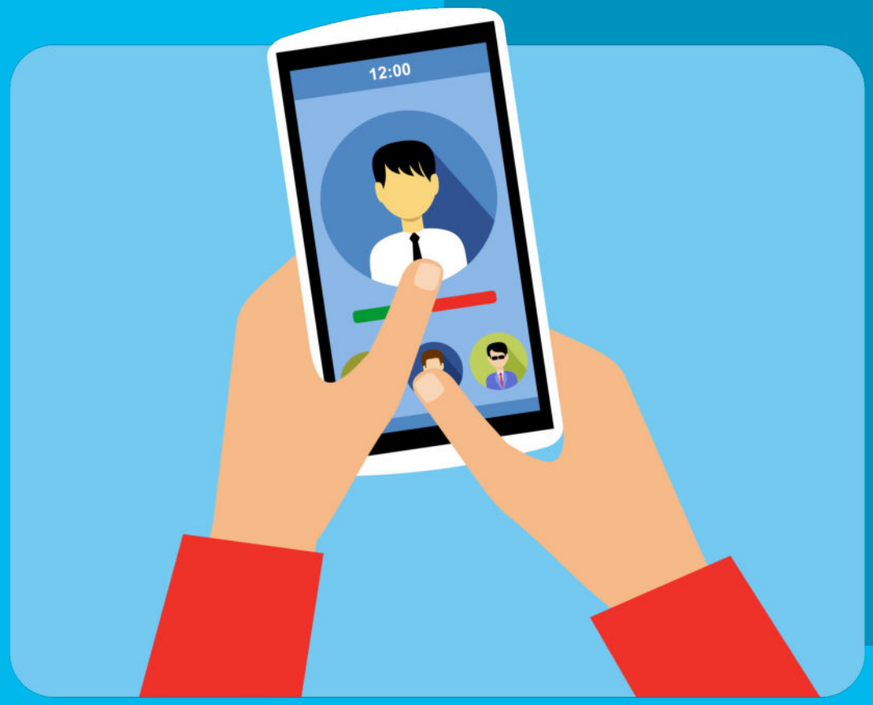
İfade özgürlüğümüzü kullanabilmek için özgür olmalıyız.

Bu kılavuz da kişilerin ifade özgürlüğünün çeşitli biçimlerini kullanırken kendilerini korumaları için temel araçlar sağlamaya yönelik bir girişimdir- ancak bu durumda bile, kişilerin hayati önem taşıyan işlerini güvenli bir şekilde yürütmelerini sağlamak için gerçekten ihtiyaç duyulan şeylerin yalnızca genel hatlarını çizmektedir.

Bu rehber, yerel aktivistler ve Privacy International ile iş birliği içinde, İngiltere Protesto Özgürlüğü Rehberi'nin Türkiye yasaları ve politikalarına göre uyarlanmasıyla oluşturulmuştur. Yasal tavsiye yerine geçmesi amaçlanmamıştır ve sadece ifade özgürlüğü güvenliği hakkında ve çevresinde bir dizi bilgiyi ortaya koymaya hizmet eder. Umuyoruz ki ifade özgürlüğünün özgür ve etkili bir biçimde kullanılabilmesi için hak savunuculuğu denizine bir damla da olsa can suyu olur.

Sosyal Medya Takibi





74z6j20n
f36rq928

TEMEL BULGULAR

- İfade özgürlüğünün kullanımı için sosyal medya önemlidir insanlar kendilerini ifade etmek için sosyal medyaya güveniyor
- Gelişen teknolojiyle birlikte insanlar teknoloji tabanlı gözetime maruz kalmaktalar, çevrimiçi faaliyetler gözetimin kilit bir taşıyıcısı olarak gözlemlenmektedir
- Bu kılavuz, bireylerin çalışmaları için gerekli araçları kullanmaya devam etmelerini sağlayabilecek hafifletici önlemler sunmayı amaçlamaktadır. Yurttaşların sosyal medya takibinden kaçınmak için kullanabilecekleri bazı bilgiler sunmak istedik, böylece kendinizi ifade etmekte daha özgür olabilirsiniz.

Çevrimiçi paylaştığınız kişisel bilgi miktarını kısıtlama

- Sosyal medya, benzer düşünen insanların bir araya gelmesinde, örgütlenmesinde ve değişimin sağlanmasında kilit bir rol oynamaktadır.
- Sosyal medya faaliyetleri, kendi ifade etmede ve sosyal konulara katılımda şüphesiz faydalı olmakla birlikte, risksiz değildir- sosyal medya platformlarındaki faaliyetler, diğer aktörlerin takip etmek veya istismar etmek isteyebileceği bir ayak izi bırakabilir. Bu nedenle kişisel bilgilerin paylaşımının kısıtlı olması faydalı olacaktır.

Sosyal medya izleme

Facebook, Twitter, Instagram ve Reddit gibi sosyal medya platformlarında paylaşılan bilgilerin izlenmesi, toplanması ve analiz edilmesi anlamına gelir. Bu tür bir izleme, genel veya özel gruplarda veya sayfalarda yayınlanan içeriğin taranmasını içerebilir. Ayrıca, yayınladığınız içerik ve davranışlarınızla ilgili veriler (neleri beğendiğiniz ve paylaştığınız gibi) dahil olmak üzere bir sosyal medya platformundan tüm verilerin alınmasını içeren "kazıma (scraping)" işlemini de içerebilir. Kazıma ve diğer araçlar yoluyla sosyal medya izleme, kullanıcılar hakkında profiller ve tahminler oluşturmak için kullanılabilecek geniş bir sosyal medya veri havuzunun toplanmasına ve analiz edilmesine izin verir.

Sosyal medya siteleriyle etkileşim şekliniz, bazen farkında olmadan hakkınızda pek çok şeyi açığa çıkarabilir ve gizlilik ayarlarınızı belirli bir şekilde değiştirmezseniz, verileriniz sosyal medya izlemesine karşı daha savunmasız hale gelir. Sosyal medya hesaplarınızda gizliliğinizi koruyabilecek ve üçüncü tarafların faaliyetlerinizi gözetlemesini zorlaştıracak genel iyi uygulamalar ve ayarlar vardır. Aşağıdaki iyi uygulama önlemleri Twitter, Facebook veya Instagram olsun tüm sosyal medya siteleri için geçerlidir.

Güvenlik

- İki faktörlü kimlik doğrulamayı etkinleştirmeyi (2FA olarak da bilinir) düşünebilirsiniz. Bu hesabınıza erişmek için ekstra bir güvenlik adımı sağlar. Bu şekilde, bağlandığınızda, sosyal medya hesabınız kullanıcı adınız ve şifrenize ek olarak bir kod isteyerek kimliğinizi doğrulayacaktır.
- Şifre sıfırlama korumasını etkinleştirmek hesabınızı ele geçirmeye çalışan kişilerin sıfırlama kodunun gönderileceği cep telefonu numaranız/mail adresiniz gibi kişisel verilerinize ulaşmasını engelleyebilir.
- Hesabınıza başka cihazlardan (herkese açık/paylaşılan) giriş yaptığınızda her seferinde oturumu kapattığınızdan emin olun.
- Kullandığınız uygulama dosya paylaşımına izin veriyorsa, size gönderilen herhangi bir şeyi indirmeden (telefonunuzda açılması gereken bir dosya veya belge gibi) veya tanımadığınız veya güvenmediğiniz kişiler tarafından gönderilen bağlantılara tıklamadan önce dikkatli olun.

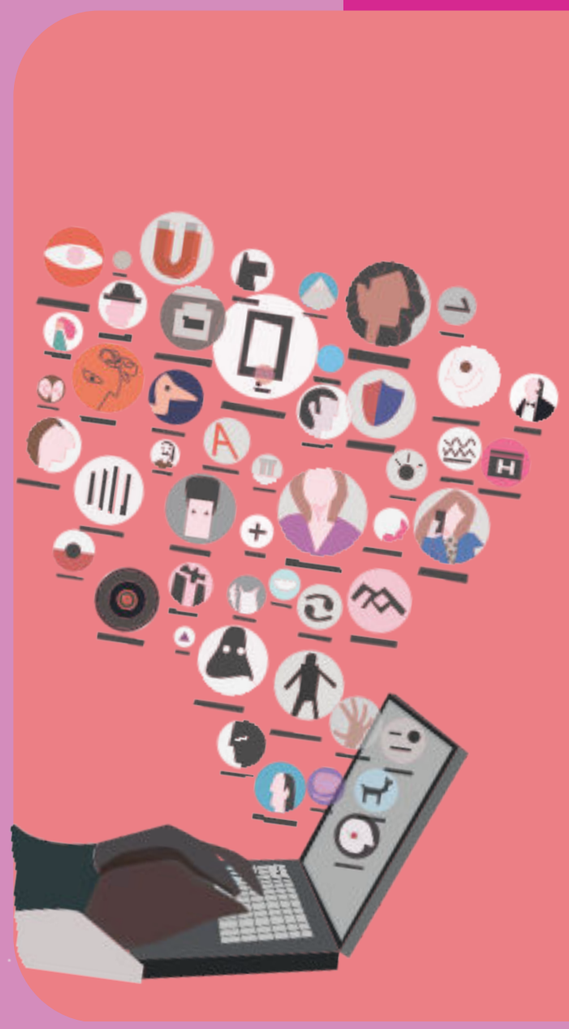
Gizlilik ayarları

- Kullandığınız sosyal medya platformlarının veya uygulamalarının gizlilik ayarlarını fırsat buldukça gözden geçirmek iyi bir fikir olacaktır. Özellikle, kullandığınız platformların veya uygulamaların üçüncü taraflarla veri paylaşıp paylaşmadığını gözden geçirmeyi ve bu tür verilerin paylaşımına izin verirken takdir yetkinizi kullanmayı düşünün.
- İzniniz olmadan kişilerin sizi fotoğraflarda etiketlemesine izin vermeyi kısıtlayan ayarları etkinleştirmeyi düşünebilirsiniz.
- Mümkün olan yerlerde gizlilik modunu etkinleştirmeyi düşünebilir ve bilinmeyen hesaplardan gelen takip istekleri kabul etmeyin.

Paylaşım yaparken nelere dikkat etmelisiniz

- Fotoğraflarınızda veya başlıklarınızda paylaştığınız hassas bilgilere dikkat edin.
- Cihazlarınızdaki konum ayarlarının farkında olun ve konumunuzun arka plan ayrıntılarıyla ortaya çıkabileceğini göz önünde bulundurun. Benzer şekilde, resimlerinizle birlikte yüklenmiş olabilecek tüm verileri gözden geçirmeyi ve gerektiğinde silmeyi veya değiştirmeyi düşünün.
- Hashtag kullanmak istiyorsanız, hakkınızda hangi özel verileri (veya konumu) ifşa edebileceklerini göz önünde bulundurun.
- Anonim kalmak istiyorsanız, doğum tarihiniz, doğum yeriniz, yaşınız, yaşadığınız yer, mesleğiniz, eğitim bilgileriniz gibi anonimliğinize zarar verecek kişisel verileriniz ile ilgili paylaşım yapmamayı düşünebilirsiniz.
- Çocukların fotoğraflarını sosyal medyada paylaşırken dikkatli olun.

Mesajlaşma – Uygulamalar ve Sosyal Medya Mesajlaşmaları





BAŞKALARIYLA İLETİŞİM KURMA REHBERİ: MESAJLAŞMA UYGULAMALARI

Mesajlaşma uygulamaları, uzaktaki akrabalarımızla iletişim kurmaktan, sosyalleşmeye, siyasete dahil olmaya kadar hayatımızın her alanında birbirimizle iletişim kurma şeklimizin önemli bir parçası haline geldi. Bu uygulamalardan bazıları Facebook Messenger, Twitter DM, Whatsapp, Signal, Telegram ve Viber'dır. Bu uygulamalar, özel sohbetler için kullanılabileceği gibi tek başına eylemlerden kitlesel toplantılar ve barışçıl protestolar düzenlemeye kadar değişen anayasal hak kullanımı için grup sohbetleri oluşturmak için kullanılabilir. Bu nedenle kişilerin güvenlikleri için bu uygulamalara duydukları güvenle orantılı olan uygulamaları kullanmaları önemlidir. Ancak o kadar çok uygulama var ki, hangilerinin en güvenli olduğunu bilmek zor.

Daha fazla bilgi edinmek için aşağıdaki kılavuzumuza göz atın:
Bir mesajlaşma uygulaması kullanırken göz önünde bulundurmanız gereken temel faktörler nelerdir?
Kullanmak istediğiniz mesajlaşma uygulamasına karar verirken göz önünde bulundurmanız gereken iki ana husus vardır:

1.İletişiminizin içeriğini koruyan uçtan uca şifreleme sunup sunmadığı; ve

2.Konum, kiminle iletişim kurduğunuz ve 'meta veri' olarak adlandırılan diğer ayrıntılar gibi mesaj içeriğinin ötesinde herhangi bir bilgi toplayıp toplamadığı.

Şifreli mesajlaşma neden önemlidir?

Şifreleme, bilginin gönderici ve hedeflenen alıcı(lar) dışında kimse tarafından okunamayacak şekilde karıştırılması işlemidir. Gizlice iletişim kurmak için kriptografinin kullanımı eski Mısır'a kadar uzanır ve günümüze kadar devam eder. Uçtan Uca Şifreleme ("E2EE"), şifrelenmiş içeriğin bir alıcıdan ("uç") diğerine, içeriği aktarım sırasında üçüncü taraflarca okunamayacak veya değiştirilemeyecek şekilde gönderilmesi sürecini tanımlar. E2EE, iletilen bilgilerin gizliliğini ve bütünlüğünü kaynakta şifreleyerek ve varış noktasında şifresini çözerek sürekli olarak korur. E2EE kullanıldığında, servis sağlayıcıların sunucularından geçerken bile şifreli kaldıkları için servis sağlayıcılar içeriğe müdahale edemez veya mesajları okuyamaz. Aslında, alıcının cihazına ulaşmadan önce aktarım sırasında mesajı kesmeye çalışan herhangi biri içeriğini okuyamaz veya değiştiremez.

E2EE, mesajların kimin yazdığını kanıtlamak için imzalandığı dijital imzaların kullanılmasıyla daha emin hale getirilir.
Neredeyse tüm mesajlaşma uygulamalarında, mesajlar alındığında telefonunuzun bunların şifresini çözeceğini, kaydedeceğini ve uygulamada şifresi çözülmüş olarak size göstereceğini unutmamak önemlidir. Ancak şifreli mesajlaşma, birisinin mesajlarınızı okumak için telefonunuza erişmesine karşı sizi mutlaka korumaz.

Bu nedenle, hassas konuşmalar için, mesajların uzun süreli depolanmasını durdurmak için bir yöntem olarak uygulamanız tarafından sunuluyorsa, kaybolan / zamanlanmış / yok olan mesajları kullanmayı düşünebilirsiniz. Bununla birlikte, bir görüşmedeki herhangi bir alıcının ekran görüntüsü alabileceğini veya mesajı başka bir şekilde saklayabileceğini de unutmamak önemlidir. Ayrıca, uygulama mesaj silme işleminin gerçekleştiğine dair bir bildirim görüntüler ve manuel olarak silinen mesajlar için yer tutucuları gösterir. Kendi kendini imha eden mesajların da cep telefonu çıkarma teknolojisi ile kurtarılıp kurtarılamayacağı belirsizdir.

Öte yandan Twitter gibi uygulamaların takip ettiğiniz kişiler ve sizi takip eden kişiler gibi platformdaki diğer kişilerle nasıl etkileşimde bulunduğunuzu, şifreli mesajlarla ilgili meta verileri ve mesajların içeriğini, alıcılar ve mesajların tarih ve saati dahil olmak üzere Direkt Mesajlara ilişkin verileri topladığını unutmayın.[1]
Kısa mesajlara/SMS'lere kıyasla sağladıkları daha yüksek güvenlik ışığında mesajlaşma için E2EE'yi düşünmek isteyebilirsiniz. SMS mesajları tamamen şifresizdir, yani kolayca okunabilir, aktarım sırasında manipüle edilebilir veya taklit edilebilirler. Ayrıca telekomünikasyon sağlayıcınız tarafından saklanabilirler ve bu da sizi gözetlemek isteyen kişilerin erişim taleplerine tabi olabilir.

[1] https://x.com/en/privacy

Uygulamanız hem içeriği hem de iletişim verilerini şifreliyor mu?

Bir uygulama seçerken göz önünde bulundurulması gereken bir diğer husus da meta veri üretimidir- bu, mesajlarınızın içeriğinden ziyade ne, kime ve ne zaman gönderdiğinizle ilgili verilerdir.
Signal, E2EE'yi yalnızca mesajların içeriğini şifrelemek için değil, aynı zamanda tüm meta verileri kendisinden bile gizlemek için kullanır ve yalnızca bir hesabın ne zaman oluşturulduğunu ve hizmete en son ne zaman bağlandığını depolar.

Buna karşın, hem WhatsApp hem de Telegram IP adresleri, profil fotoğrafları, "sosyal grafikler" ve daha fazlası dahil olmak üzere çok daha fazla meta veri depolar ve bunlara erişebilir.
Telegram'ın durumunda, Telegram varsayılan olarak E2EE kullanmaz, bunun yerine tüm mesajları üzerinde tam kontrole sahip oldukları anahtarlarla saklar. Sonuç olarak, Telegram mesajlara her an erişim sağlayabilir. Hem WhatsApp'ın hem de Telegram'ın polisin bilgi taleplerine zaman zaman yanıt verdiği vakalar sağlayıcı şirketlerin bu mesajlaşmalara erişimleri olduğunu göstermektedir.
WhatsApp ayrıca başkalarıyla nasıl etkileşim kurduğunuzun yanı sıra gruplar veya arama gibi kullandığınız özellikler gibi bilgileri de toplar, ancak Signal gibi şifrelenmiş mesajları teslim edildikten sonra sunucularında tutmazlar ve teslim edilmeyen mesajları 30 gün sonra silerler.

Uygulamanız, kullanmak için telefon numaranızı gerektirebilir

Kayıt sırasındaki adım sayısını azaltmak için çoğu mesajlaşma uygulaması bir telefon numarasına dayanır. Bu daha yaygın kullanım için faydalı olsa da, kişisel numaralarını vermek istemeyen kişiler için ideal olmayabilir.
Bundan kaçınmanın yolları vardır, örneğin sahip olduğunuz alternatif bir SIM kartın numarasını kullanarak mesajlaşma uygulamasına kaydolmak gibi.

Metadata

Farklı uygulamalar meta verilerin depolanması ve saklanması konusunda farklı yaklaşımlar uyguladığından, meta veriler uygulama seçiminde dikkate alınması gereken bir diğer hususdur.
Meta veriler mesajlarınızın içeriği kadar açıklayıcı olabilir. Meta veriler, iletişimin içeriğinden ayrı olarak bir iletişim hakkındaki tüm bilgilerdir. Örneğin, bir cep telefonu görüşmesi için, hangi numarayı aradığınız, aradığınızda nerede olduğunuz, saat kaçta aradığınız ve görüşmenin ne kadar sürdüğü gibi bilgileri içerir.
Signal E2EE'yi yalnızca mesajların içeriğini şifrelemek için değil, aynı zamanda tüm meta verileri kendisinden bile gizlemek için kullanır ve yalnızca bir hesabın ne zaman oluşturulduğunu ve hizmete en son ne zaman bağlandığını saklar. Buna karşılık, hem WhatsApp hem de Telegram IP adresleri, profil fotoğrafları, "sosyal grafikler" ve daha fazlası dahil olmak üzere çok daha fazla meta veri depolar ve bunlara erişebilir.

Mesajlaşma uygulamanızda paylaşılan bilgileri daha iyi kontrol etmek için göz önünde bulundurmanız gereken ek önlemler

Uçtan uca şifrelenmiş bir mesajlaşma uygulaması seçseniz de seçmeseniz de, uygulamada paylaştığınız bilgilerin güvenliğini sağlamak için ek adımlar atmayı düşünebilirsiniz.

Sohbet yedekleme

Bazı uygulamalar sohbet yedeklemeyi bir seçenek olarak sunabilir. Mesajlarının kaybolmasını önlemek için yedekleme birçok kişi için arzu edilir olsa da, Bulut üzerinde yedekleme, Apple (iCloud'da yedeklenmişse) veya Google hesabınıza (Android'de yedeklenmişse) erişimi olan herhangi biri erişebileceğinden, kullanıcıların gizliliği için potansiyel bir tehdit oluşturabilir.
Yedek tutmamayı tercih ederseniz, bu, mesajlarınızın yalnızca uygulama içinde var olduğu anlamına gelmelidir, bu da saldırı yüzeyini en aza indirir.

Profil bilgilerinizi en aza indirin

Mesajlaşma uygulamaları genellikle bir fotoğraf, bir durum veya bir 'hakkında' bölümü içerebilen bir profil tutmanıza olanak tanır.
Güvenmediğiniz kişilerle iletişim kurmayı düşünüyorsanız, bu bilgiler sizin hakkınızda gizli kalmasını istediğiniz şeyleri açığa çıkarabilir.
Genel bir kural olarak, sunulan en özel seçeneği seçmeyi düşünebilirsiniz.
Çoğu durumda, bu ayrıntıların görünürlüğünü "kişilerinizle" sınırlamak iyi bir seçenek olabilir, ancak mesajlaşma uygulamasını tanımadığınız kişilerle bağlantı kurmak için kullanmayı düşünüyorsanız, herhangi bir profil ayarını minimumda veya boş tutmaya değer olabilir.

Uygulama	E2EE Teklifleri	Varsayılan Olarak E2EE	Telefon numarası gerektirir
iMessage	Evet	Bulutta depolanmadığında	Evet
WhatsApp	Evet	Evet	Evet
Signal	Evet	Evet	Evet
Viber	Evet	Evet	Evet
Telegram	Biraz	Hayır	Evet
Skype	Evet	Hayır	Hayır
Wickr	Evet	Evet	Hayır
Matris Müşteri	Müşteri Bazlı	Müşteri tarafından teklif edildiğinde	Hayır
Facebook Messanger	Evet	Hayır	Giderek artan bir şekilde
Google Mesajları	Evet	Evet	Hayır
Instagram DM'leri	Evet	Hayır	Hayır
Twitter DM'leri	Hayır	Hayır	Giderek artan bir şekilde
Discord	Hayır	Hayır	Hayır

GÖZETİMDEN KAÇINMA



CEP TELEFONU ÇIKARMA İŞLEMİ NASIL KULLANILABİLİR VE VERİLERİNİZE YÖNELİK RİSKLERİ NASIL EN AZA İNDİREBİLİRSİNİZ

Cep telefonu çıkarma araçları ne işe yarar?

• Cep telefonu çıkarma (MPE) araçları, cep telefonlarından aşağıdakiler de dahil olmak üzere veri çıkarmasına olanak tanıyan cihazlardır:
- kişiler;
- arama verileri (yani kimi, ne zaman ne kadar süreyle aradığınız)
- metin mesajları (kime ve ne zaman mesaj attığınız dahil);
- depolanan dosyalar (fotoğraflar, videolar, ses dosyaları, belgeler vb;)
-uygulama verileri (bu uygulamalarda depolanan veriler dahil);
- konum bilgisi geçmişi;
- wifi ağ bağlantıları (bunlar iş yeriniz veya bir kafe gibi wifi'ye bağlandığınız herhangi bir yerin konumunu ortaya çıkarabilir).

• Bazı MPE araçları Bulutta depolanan verilere de erişebilir (bu nedenle cihazınızda depolanan verileri en aza indirme konusunda çok dikkatli olsanız bile, çevrimiçi olarak depolanmışsa yine de erişilebilir) veya varlığından bile haberdar olmadığınız verilere ve hatta silinmiş verilere bile erişebilir.



Nelere dikkat etmelisiniz?

• Telefonunuzun işletim sistemini (Android veya iOS) güncel tutmak, yani en son güvenlik özelliklerine sahip olmak, muhtemelen MPE'yi önlemenin en iyi yoludur.

• MPE'ye karşı kendinizi korumanın en etkili yolu telefonunuzu güvensiz olabileceğiniz yerlere götürmemek olsa da, bunun gerçekçi bir çözüm olması pek olası değildir. Aslında, telefonunuzu yanınızda bulundurmamak sizi başka şekillerde savunmasız bırakabilir.

• Telefonunuzu kilitli tutmanız gerekirken, bazı MPE araçlarının kilitli telefonlara bile erişmek üzere tasarlandığı bildirilmektedir. Ancak bu araçların bu güvenliği aşma kabiliyeti telefona ve işletim sistemine bağlıdır.

• Telefon verilerinizi bilgisayarınıza yedeklemeyi ve ardından bu verileri telefonunuzdan kaldırmayı düşünebilirsiniz. Ancak bazı MPE araçlarının silinen verileri kurtarabildiğini bilmelisiniz. Verileri bir bulut hizmetine kaydettiyseniz, bazı MPE araçları bu verilere yine de erişebilir.

'BULUTTAN ÇIKARMA' ARAÇLARI NASIL KULLANILABİLİR VE VERİLERİNİZE YÖNELİK RİSKLERİ NASIL EN AZA İNDİREBİLİRSİNİZ

'Bulut çıkarma araçları' nedir ve ne işe yarar?

• Bulut çıkarma teknolojisi, cep telefonunuz veya diğer cihazlarınız aracılığıyla 'Bulut'unuzda depolanan verilere erişmesini sağlar.
• Bulut çıkarma araçlarının kullanılması, yetkisiz kişilerin çevrimiçi olarak sakladığınız verilere erişebileceği anlamına gelir. Bulutta veri depolayan uygulamalara örnek olarak Slack, Instagram, Telegram, Twitter, Facebook ve Uber verilebilir.

Nelere dikkat etmelisiniz?

• Güvensiz bir ortamdaysanız telefonunuzda kullandığınız uygulamalarda bulut yedeklemeyi kapatmayı ve tüm bulut tabanlı hizmetlerden çıkış yapmayı düşünmelisiniz. Bu, verilerin Bulutta depolanmasını ve cep telefonunuzdan bu verilere erişimi önleyecektir.
• Uçtan uca şifrelenmiş mesajlaşma kullansanız bile örneğin WhatsApp aracılığıyla, WhatsApp mesajlarınızı Bulut'a yedeklerseniz, bu şifrelenmiş yedeklere telefonunuzdaki bulut çıkarma araçları kullanılarak erişilebilir.
• Uber, Twitter, WhatsApp ve Facebook gibi bazı uygulamalar Bulutta saklanan konum verilerini kapatmanıza izin verir. Bu, yetkisiz kişilerin bulunduğunuzu izlemesini engelleyebilir.

IMSI YAKALAYICILARI NASIL KULLANILABİLİR VE VERİLERİNİZE DAİR RİSKLERİ NASIL EN AZA İNDİREBİLİRSİNİZ

IMSI Yakalayıcı nedir?

IMSI', SIM kartınıza özgü bir numara olan 'uluslararası mobil abone kimliği' anlamına gelir. IMSI yakalayıcılar 'Vatozlar' olarak da bilinir.

• Bir 'IMSI yakalayıcı', benzersiz IMSI numarasını 'yakalayarak' çevresindeki bir telefon ağına bağlı tüm cep telefonlarının yerini belirleyen ve ardından izleyen bir cihazdır.

• Bunu, bir cep telefonu kulesi gibi davranarak, yakındaki cep telefonlarını kendisine bağlanmaları için kandırarak yapar ve daha sonra telefon kullanıcısının bilgisi olmadan o telefondan baz istasyonuna giden verileri kesmesini sağlar.

• Bu durumda hakkınızdaki en erişilebilir bilgi konumunuzdur. Baz istasyonlarının üçgenleme yoluyla kabaca konumunuzu bilmesi kaçınılmazdır- aslında size ilk etapta bu şekilde hizmet sağlar. Bir IMSI yakalayıcı, sizinle baz istasyonu arasına girerek kabaca konumunuzu tespit edebilir.

• IMSI yakalayıcılar telefonda depolanan verileri okumaz. Bunun yerine, bu cihazlar kısa mesajları ve telefon görüşmelerini engellemeye çalışmak için kullanılabilir.

• IMSI yakalayıcının yeteneklerine ve telefonunuzun bağlandığı ağa bağlı olarak, daha gelişmiş saldırılar gerçekleşebilir, ancak bu pek olası değildir. Bazı Stingray cihazları, iletişim protokollerinin bilinen zayıflıklarından yararlanır ve telefonunuzu kullandığı protokolleri düşürmeye zorlayarak iletişiminizi daha az güvenli ve daha kolay erişilebilir hale getirebilir (örneğin, 3G üzerinden iletişimi 2G'ye düşürerek, çünkü bildiğimiz kadarıyla, içerik müdahalesi ve gerçek zamanlı şifre çözme yalnızca hedef 2G ağı üzerinden bağlandığında gerçekleştirilebilir).

• IMSI yakalayıcılar, uçtan uca şifreleme kullanan platformlar (örneğin Signal, WhatsApp, Wire) aracılığıyla paylaştığınız şifreli mesajların içeriğini okuyamaz.



Nelere dikkat etmelisiniz?

• Telefonunuzu uçak moduna almak veya tamamen kapatmak, IMSI yakalayıcının sizi veya iletişiminizi takip edemeyeceği anlamına gelecektir.

• Metin mesajlarınızın içeriğinin bir IMSI yakalayıcı tarafından izlenmesini önlemek istiyorsanız, Signal ve WhatsApp gibi uçtan uca şifreleme kullanan mesajlaşma hizmetlerini kullanabilirsiniz. Bir IMSI yakalayıcısının potansiyel olarak toplayabileceği tek bilgi, içeriğin kendisi değil, bu mesajlaşma uygulamalarını kullandığınız gerçeğidir.

• IMSI yakalayıcılar telefonda depolanan verileri okumasa da kötü niyetli kişilerin telefonunuzdaki verilere erişmelerini sağlayan 'cep telefonu çıkarma' ve bilgisayar korsanlığı araçları gibi başka teknolojilere sahip olabileceğini unutmayın.

1.

HACKLEME NASIL KULLANILABİLİR VERİLERİNİZE YÖNELIK RİSKLERİ EN AZA NASIL İNDİREBİLİRSİNİZ

Hackleme (Bilgisayar korsanlığı) nedir?

• Hackleme, ya elektronik sistemlerdeki güvenlik açıklarını bulmak, bunları rapor etmek ve onarmak ya da bunlardan yararlanmak anlamına gelir.

• Hackleme, milyonlarca insanın kullanabileceği cihazlar, ağlar ve hizmetlerdeki güvenlik açıklarının tespit edilmesine ve düzeltilmesine yardımcı olabilir. Ancak cihazlarımıza erişmek, hakkımızda bilgi toplamak ve bizi ve cihazlarımızı başka şekillerde manipüle etmek için de kullanılabilir.

• Hackleme sürekli gelişen bir dizi teknikten oluşur. Uzaktan yapılabilir, ancak bir cihaza veya sisteme fiziksel müdahaleyi de içerebilir- örneğin bir cep telefonunun kilidini açmaya zorlayarak.

• Ayrıca insanların teknolojilerine erişim sağlamak için onlardan faydalanmayı da içerebilir. Bir saldırganın güvenilir bir kişi ya da kuruluşun kimliğine bürünerek kötü amaçlı yazılım bulaşmış bir bağlantı ya da ek göndermesi 'oltalama (phishing)' yöntemine örnek olarak verilebilir.

Hackleme (bilgisayar korsanlığı) iletişimde nasıl kullanılabilir?

• Hackerlar, örneğin 'IMSI yakalayıcıları' kullanarak iletişimi hackleyebilir. Ancak IMSI yakalayıcılar yalnızca bir mobil cihaz ile baz istasyonu arasında iletilen bilgilere müdahale edebilir; IMSI yakalayıcılar cihazda depolanan bilgilere erişemez.

• Dolayısıyla, bir şifre, parmak izi ya da yüz kilidi ile güvence altına alınmış olsalar bile, bir telefon, dizüstü bilgisayar ya da diğer internet bağlantılı cihazlarda depolanan bilgilere uzaktan erişim sağlamak için sofistike bilgisayar korsanlığı tekniklerini kullanabilir.

• Ayrıca düşürülen, kaybedilen vb. cihazlar kötü niyetli kişilerin eline geçebilir ve bunlara erişim sağlanabilir.

Nelere dikkat etmelisiniz?

Cihazınızı güncel tutmak, hacklenmeyi önlemenin iyi bir yoludur, çünkü hackleme genellikle açıklanmış ancak henüz yamalanmamış güvenlik açıklarından yararlanır.

Güvenliğinizi artırmak ve hacklenme riskini en aza indirmek için cihazınızın işletim sisteminin (Android veya iOS) mevcut en son sürümünü çalıştırdığından ve tüm uygulamalarınızın güncel olduğundan emin olun.

Telefonunuzu veya diğer elektronik cihazlarınızı kilitli tutmanız gerekirken, bazı hackleme teknikleri kilitli cihazlara bile erişebilir. Ancak bu güvenliği aşma becerileri, kullanılan hack tekniğine ve hedef aldığı cihaza bağlıdır.

Güvende olmadığınızı düşündüğünüz bir yere gitmeden veya bir ağa bağlanmadan önce, telefon verilerinizi başka bir cihaza yedeklemeyi ve ardından bu verileri yanınızda götürdüğünüz cihazlardan kaldırmayı düşünebilirsiniz. Ancak bazı hackleme araçlarının silinen verileri kurtarabildiğini bilmelisiniz. Verileri bir bulut hizmetine kaydettiyseniz, bazı bilgisayar korsanlığı araçları bu verilere yine de erişebilir.

'Oltalama' saldırılarından kaçınmak için hangi bağlantılara tıkladığınız konusunda her zaman dikkatli olmalısınız.

FİZİKİ GÖZETİM









VÜCUDA TAKILAN KAMERALAR

Vücuda Takılan Video kameralar ne işe yarar?

• Vücuda Takılan Video (BWV) kameralar bir kişinin kıyafetine- genellikle göğüs, omuz veya baş hizasına veya yakaya- takılabilir ve takan kişinin bakış açısından ses de dahil olmak üzere video kaydı yapar.

• BWV kameraları muhtemelen sizin tarafınızdan görülebilecektir ve kayıt yaparken cihaz üzerinde yanıp sönen bir ışık görünmelidir.

Vücut kameraları nasıl kullanılabilir?

• BWV kameraları kişilerin hareketlerini yakından izlemek için kullanılabilir. Barışçıl protestolarda kolluğun ya da özel güvenliklerin kullandığına ilişkin vakalar mevcuttur.

• Kişinin, kendisine karşı işlenen ve başka türlü ispat imkanı olmayan suçlarla ilgili delil amacıyla kayıt almak gibi istisnai haller dışında Türk Ceza Kanunu 134. Madde gereği gizli BWV kamera kayıtları yasadışıdır.[1] Üstelik KVKK'ya aykırıdır.

• Kolluğun kullandığı BWV kamera kayıtlarının yasaya uygun olması için kullanılmadan önce yasa gereği görüntüsü ve sesi kaydedilecek kişinin "görüntü ve ses kaydı" alınacağına ve ne için kullanılacağına dair bilgilendirilmesi gerekmektedir.

• Görüntüler daha sonra, örneğin yüz tanıma yazılımı tarafından işlenebilir.

[1] TCK 134/1 Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır.



GÖZETİME KARŞI ARAÇLARINIZI KORUMA REHBERİ



KONUM VERİLERİNİZE ERİŞİMİ NASIL DAHA İYİ KONTROL EDEBİLİRSİNİZ

Telefonumun konum verileri nerede saklanıyor?

Telefonunuzun konumu GPS veya mobil ağ konumu kullanılarak iki ana yolla belirlenebilir:

1. GPS

- GPS (Küresel Konumlandırma Sistemi anlamına gelir), telefonunuzun yerini oldukça hassas bir şekilde (birkaç metre içinde) belirlemek için uydu navigasyonunu kullanır ve telefonunuzun içindeki bir GPS çipine dayanır.
- Kullandığınız telefona bağlı olarak GPS konum verileriniz yerel olarak ve/veya Google Cloud veya iCloud gibi bir bulut hizmetinde depolanabilir. GPS konumunuza erişimi olan kullandığınız herhangi bir uygulama tarafından da toplanabilir.

2. Mobil ağ konumu

- Mobil ağ konumu (veya Mobil İletişim için Küresel Sistem (GSM) konum belirleme) hücresel ağınıza dayanır ve ağa bağlandığınız anda (yani telefonunuz açık ve uçak modunda değilken) belirlenebilir, ancak GPS'ten çok daha az hassastır. Yaklaşık konumunuz, bir şehirde onlarca metre veya kırsal alanlarda yüzlerce metrelik bir doğruluk aralığında belirlenebilir.
- Bu konum verileri şebeke sağlayıcınız tarafından saklanır.
- Konumunuzu dolaylı olarak belirlemek için açık wifi erişim noktaları ve telefonlarınızın bağlandığı Bluetooth işaretçileri veya fotoğraflarınıza gömülü konum meta verileri gibi başka yöntemler de kullanılabilir.

Konum verilerime nasıl erişilebilir?

Başka kişilerin (telefonunuzun) konumuna erişmek için kullanabileceği birkaç yöntem vardır:

1. GPS

- GPS konum verilerine erişim, verilerin nerede depolandığına bağlıdır. Telefonunuza takılan ve ziyaret ettiğiniz yerlerin ayrıntıları da dahil olmak üzere telefonunuzda depolanan tüm verileri indiren bir 'cep telefonu çıkarma' cihazı kullanılarak yapılabilir.
- GPS verilerinize erişim, telefonunuza fiziksel erişim gerektirmeyen ve uzaktan yapılabilen gelişmiş bir teknik olan cihaz korsanlığı yoluyla da mümkün olabilir.
- GPS verileriniz çevrimiçi bir hesapta da saklanıyorsa (örneğin iCloud veya Google Maps), bulut ayıklama teknolojileri veya bu verileri saklayan şirketlere yapılan yasal talepler yoluyla bu verilere erişilebilir.
- GPS verilerinize servis sağlayıcınız aracılığıyla erişilebilir.

2. Mobil ağ konumu

- Yaklaşık konum verilerinize servis sağlayıcınız aracılığıyla erişilebilir.
- Aynı bilgilere erişmenin bir başka yolu da, belirli bir bölgede açık olan ve bir mobil ağa bağlı olan tüm cep telefonlarını yakalamak ve izlemek için kullanılan bir cihaz olan 'IMSI yakalayıcı' ('Stingray' olarak da bilinir) kullanmaktır.

Konum verilerinizi nasıl daha iyi kontrol edebilirsiniz?

1. GPS

- Konumunuza erişilmesini önlemenin en iyi yolu, ilk etapta konum verilerinin oluşturulmasını sınırlamaktır.

- GPS söz konusu olduğunda, bu GPS'inizi kapatmak kadar basit olabilir (genellikle 'konum hizmetleri' olarak adlandırılır). Ancak daha önce GPS'i açık tuttuğunuz durumlardaki konum verilerinin hala erişilebilir olabileceğini unutmayın.

- Telefonunuzda hala GPS kullanmanız gerekiyorsa, bu bilgilerin yayılmasını en aza indirmek için uygulamaların konumunuza erişim izinlerini tek tek kontrol edin.

- Tüm uygulamalar için konumunuza erişim izinlerini kaldırmak, bu verilerin çevrimiçi bir hesapta depolanmasını önleyebilir.

- Bir uygulamanın GPS verilerinize erişmesine kesinlikle ihtiyacınız varsa, konumunuzun çevrimiçi olarak mı yoksa yalnızca uygulamanızda yerel olarak mı depolandığını anladığınızdan emin olmak için söz konusu uygulamanın ayarlarını inceleyin. Örneğin, bir Google hesabında oturum açmışken Google Haritalar'ı kullanıyorsanız, konum geçmişinizin Google hesabınızda saklanmaması için ayarlardan konum geçmişini devre dışı bırakmak isteyebilirsiniz.

- Konum hizmetleriniz açıkken fotoğraf çektiyseniz, resmin çekildiği konum resmin meta verilerine (EXIF verileri olarak bilinir) dahil edilebilir. Fotoğraf çekerken konum hizmetlerini devre dışı bırakmak isteyebilirsiniz veya daha sonra bu EXIF verilerini silmek için bir yazılım veya uygulama kullanabilirsiniz (örneğin, Signal mesajlaşma uygulaması görüntü gönderdiğinizde EXIF verilerini siler).

- Benzer şekilde, wifi veya Bluetooth'unuzu kapatarak telefonunuzun istenmeyen erişim

2. Mobil ağ konumu

- Mobil ağ konumu söz konusu olduğunda, bunu kontrol etmenin tek yolu ağa bağlanmayı tamamen engellemektir.

- Telefonunuzun kapalı, uçak modunda veya bir faraday kafesinde olması mobil ağınıza bağlantıyı engelleyecek ve bu nedenle GSM coğrafi konumunu imkansız hale getirecektir. Faraday kafesi ya da telefonunuzu kapatmak herhangi bir telefon şebekesine her türlü bağlantıyı engeller. Oysa sadece uçak modunu kullanmak bazı bağlantı türlerinin hala yapılabileceği anlamına gelir (örneğin Bluetooth veya GPS).

TELEFONUNUZUN RESİMLERİNE, KİŞİLERİNE, BELGELERİNE NASIL ERİŞİLEBİLİR VE SİZ ERİŞİMİ DAHA İYİ NASIL KONTROL EDEBİLİRSİNİZ



Resimlerim, kişilerim ve belgelerim nerede saklanıyor?

- Telefonunuzu her kullandığınızda veri üretirsiniz; örneğin fotoğraf çektiğinizde veya video kaydettiğinizde, hareket halindeyken notlar ve belgeler oluşturduğunuzda veya düzenlediğinizde ve rehberinize yeni isimler ve numaralar eklediğinizde veri üretirsiniz.

- Tüm bu veriler özel uygulamalar aracılığıyla oluşturulur- kamera ve fotoğraf uygulamalarınız, sosyal medya uygulamalarınız, not uygulamalarınız ve kişiler uygulamanız sadece birkaç örnektir.

- Telefonunuzda herhangi bir dosya oluşturduğunuzda, genellikle ona bağlı 'meta veriler' de oluşturursunuz (örneğin, bir fotoğrafın çekildiği zaman ve yer gibi meta verileri olacaktır). Bu meta veriler, fotoğrafın kendisi kadar, hatta ondan daha açıklayıcı olabilir.

- Tüm bu veriler telefonunuzun dahili belleğinde (MicroSD kart gibi takılı harici bellekler de dahil olmak üzere) veya Bulutta ya da yedekleme olarak herhangi bir bulut hizmeti kullanıyorsanız her ikisinde birden saklanacaktır.

Görüntülerime, kişilerime ve belgelerime nasıl erişilebilir?

Nasıl saklandıklarına bağlı olarak bu verilere erişilebilmesinin birkaç yolu vardır:

- Tüm verilerinizi telefonunuzda yerel olarak saklıyorsanız, telefonunuza bağlanan ve içinde saklanan tüm verileri indiren bir 'cep telefonu çıkarma' cihazı kullanılarak erişilebilir. Bu yöntem uzaktan kullanılamaz- bu verilere erişmek isteyen kişilerin telefonunuza fiziksel erişime ihtiyacı olacaktır.

- Cihaz korsanlığı, telefonunuzdaki belirli miktarda veriye erişim sağlayan, ancak hepsine erişmek zorunda olmayan gelişmiş bir tekniktir. Cep telefonu çıkarmanın aksine, cihaz korsanlığı cihazınıza fiziksel erişim gerektirmez. Bu, bu yöntemin bir protestodan önce veya sonra herhangi bir zamanda kullanılabileceği anlamına gelir.

- Görüntülerinizi, belgelerinizi ve kişilerinizi herhangi bir bulut hizmeti (örneğin iCloud, Dropbox veya Google Drive) kullanarak senkronize ediyorsanız, kötü niyetli kişiler bu bilgilere izniniz veya bilginiz olmadan erişmek için uzaktan 'bulut çıkarma' araçlarını kullanabilir veya bulut hizmeti sağlayıcısına yasal bir talepte bulunabilir.

Resimlerinize, kişilerinize ve belgelerinize erişilmesi riskini nasıl sınırlandırabilirsiniz?

- Bulut çıkarma teknikleri tarafından hedef alınmayı önlemek için Bulut hizmetlerini kullanmaktan tamamen kaçınmaya ihtiyacınız olabilir.

- Bulut hizmetlerinden tamamen vazgeçmek sizin için çok fazla rahatsızlık yaratacaksa, hassas içerikleri Bulut'a yüklememeyi düşünün. Uygulamaların ayarlarını ve özelliklerini gözden geçirmek de telefonunuzdaki hangi verilerin çevrimiçi olarak yedeklendiğini bilmeniz için iyi bir yoldur (örneğin, WhatsApp yedekleri Google Drive'da saklanabilir, bu nedenle WhatsApp mesajlarınız uçtan uca şifrelenmiş olsa bile, bulut çıkarma araçları kullanılarak bu mesajlara Google Drive yedeklemenizden erişilebilir).

- Bununla birlikte, cihaz kullanıcısı olarak, ilk etapta oluşturduğunuz veriler ve bunların nerede depolandığı üzerinde bir miktar kontrole sahipsiniz. Telefonunuzun sizin hakkınızda hangi bilgileri tuttuğunu iyi anlamanız, bu tür araçların telefonunuzda kullanılması durumunda hangi verilere erişildiğinin farkında olma olasılığınızın daha yüksek olduğu anlamına gelir.

- Telefonunuzun içeriğinin şifrelenmiş olduğundan ve işletim sisteminizin ve uygulamalarınızın güncel olduğundan emin olmak, bazı cep telefonu çıkarma ve cihaz hackleme yöntemlerine karşı hafifletecektir.

DİJİTAL İLETİŞİMİNİZE NASIL ERİŞİM SAĞLANABİLİR VE SİZ ERİŞİMİ DAHA İYİ NASIL KONTROL EDEBİLİRSİNİZ

İletişimlerim nerede saklanıyor?

- Metin mesajları/telefon görüşmeleri:

Geleneksel cep telefonu iletişimi hücresel ağ üzerinden gerçekleşir. Bunlara genellikle telefonunuzda standart olarak sunulan kısa mesaj ve telefon görüşmesi uygulamaları ile erişirsiniz. Telefon aramaları hiçbir yerde saklanmazken, kısa mesajlar sizin ve alıcının cihazlarında yerel olarak saklanır. Şebeke sağlayıcısı tarafından da geçici olarak saklanabilirler.

- Sosyal ağlar:

Merkezi olmayan/kendi kendine barındırılan sistemlerin nadir durumları dışında, sosyal ağ uygulamalarındaki iletişimleriniz hizmet sağlayıcılar tarafından saklanacaktır.

- Mesajlaşma uygulamaları:

Mesajlaşma platformları internet üzerinden oldukça güvenli iletişim sağlar. Kullandığınız uygulamaya bağlı olarak, mesajlarınız sizin ve alıcının telefonunda yerel olarak, servis sağlayıcının sistemlerinde ve potansiyel olarak çevrimiçi olarak da saklanabilir. Bazı mesajlaşma uygulamaları ayrıca yedekleme çözümleri de sunar ve bu yedekler ya çevrimiçi veya yerel olarak. Farklı mesajlaşma uygulamaları da farklı protokollere dayanır, bu da bazı mesajlaşma uygulamalarının diğerlerine göre daha fazla dış müdahale riski altında olduğu anlamına gelir.

İletişimlerime başka kişiler tarafından nasıl erişilebilir?

Nerede sakladığınıza bağlı olarak başka kişilerin bu verilere erişebilmesinin birkaç yolu vardır:

- Telefonunuzda depolanan iletişimlere (bir metin mesajlaşma uygulamasındaki konuşmalarınız gibi) erişmek, telefonunuzda depolanan tüm verileri indirmek için telefonunuza bağlanabilen bir 'cep telefonu çıkarma' cihazı aracılığıyla yapılabilir.

- Bu tür bir erişim, telefonunuza fiziksel erişim gerektirmeyen bir teknik olan cihaz korsanlığı ile de mümkün olabilir.

- İletişiminiz bir servis sağlayıcıya ya da bir sosyal ağa (Messenger, Telegram, Instagram, TikTok gibi) bağlıysa, başka kişiler izniniz ya da bilginiz olmadan 'bulut çıkarma' teknolojileri aracılığıyla erişim sağlayabilir. Aynı teknik, iletişiminizin yedeklerine erişmek için de kullanılabilir (örneğin Google Drive/iCloud'daki WhatsApp yedekleri).

- Kısa mesajlarınız ve telefon görüşmeleriniz, belirli bir bölgede açık ve şebekeye bağlı tüm cep telefonlarını izlemek için kullanılan bir cihaz olan 'IMSI yakalayıcı' kullanılarak başka kişiler tarafından ele geçirilebilir, kaydedilebilir ve müdahale edilebilir.

- Kısa mesajlarınıza, servis sağlayıcınızı hedef alan yasal bir süreç yoluyla da erişilebilir. Benzer yasal süreçler, iletişimlerinizi barındırabilecek şirketlerden veri talep etmek için de kullanılabilir (örneğin Twitter, Facebook).

- Ayrıca şüphelisi olduğunuz bir soruşturma varsa hakkınızda mahkeme tarafından verilmiş bir telekomünikasyon yoluyla iletişimin denetlenmesi kararı kararı ile kolluk tarafından erişilebilir iletişiminiz çeşitli teknolojilerle yasal olarak denetlenebilir. Bu denetleme karardan sonrasını kararda belirtilen süre boyunca kapsayacaktır.

İletişimlerime başka kişiler tarafından nasıl erişilebilir?

Nerede sakladığınıza bağlı olarak başka kişilerin bu verilere erişebilmesinin birkaç yolu vardır:

- Telefonunuzda depolanan iletişimlere (bir metin mesajlaşma uygulamasındaki konuşmalarınız gibi) erişmek, telefonunuzda depolanan tüm verileri indirmek için telefonunuza bağlanabilen bir 'cep telefonu çıkarma' cihazı aracılığıyla yapılabilir.
- Bu tür bir erişim, telefonunuza fiziksel erişim gerektirmeyen bir teknik olan cihaz korsanlığı ile de mümkün olabilir.
- İletişiminiz bir servis sağlayıcıya ya da bir sosyal ağa (Messenger, Telegram, Instagram, TikTok gibi) bağlıysa, başka kişiler izniniz ya da bilginiz olmadan 'bulut çıkarma' teknolojileri aracılığıyla erişim sağlayabilir. Aynı teknik, iletişiminizin yedeklerine erişmek için de kullanılabilir (örneğin Google Drive/iCloud'daki WhatsApp yedekleri).
- Kısa mesajlarınız ve telefon görüşmeleriniz, belirli bir bölgede açık ve şebekeye bağlı tüm cep telefonlarını izlemek için kullanılan bir cihaz olan 'IMSI yakalayıcı' kullanılarak başka kişiler tarafından ele geçirilebilir, kaydedilebilir ve müdahale edilebilir.
- Kısa mesajlarınıza, servis sağlayıcınızı hedef alan yasal bir süreç yoluyla da erişilebilir. Benzer yasal süreçler, iletişimlerinizi barındırabilecek şirketlerden veri talep etmek için de kullanılabilir (örneğin Twitter, Facebook).
- Ayrıca şüphelisi olduğunuz bir soruşturma varsa hakkınızda mahkeme tarafından verilmiş bir telekomünikasyon yoluyla iletişimin denetlenmesi kararı kararı ile kolluk tarafından erişilebilir iletişiminiz çeşitli teknolojilerle yasal olarak denetlenebilir. Bu denetleme karardan sonrasını kararda belirtilen süre boyunca kapsayacaktır.

İletişimlerinize erişilmesi riskini nasıl sınırlandırabilirsiniz?

Riskleri sınırlamak, paylaştığınız bilginin miktarını ve türünü, kiminle ve hangi araçla paylaştığınızı kontrol etmekle başlar.

- Çok hassas bilgileri paylaşırken yüz yüze görüşmeyi düşünün.
- Yüz yüze görüşmek bir seçenek değilse, hücresel ağların düşük güvenliği göz önüne alındığında, uçtan uca iletişim gibi güvenli kanalların kullanımını düşünün hassas bilgileri paylaşmak için şifreli mesajlaşma uygulamaları.
- Ancak mesajlaşma uygulamalarınızdan herhangi biri için bulut yedekleme kullanıyorsanız, içeriğe bulut ayıklama araçları kullanılarak erişilebileceğini unutmayın.

VPN KILAVUZU



VPN KULLANIMI İÇİN BİR KILAVUZ

Günümüzde dünyada hükümetler ve/veya kötü niyetli kişi ve kurumlar web sitelerini insanların çevrimiçi faaliyetlerini gözetlemek, engellemek de dahil olmak üzere Web'e erişim üzerinde kontrol uygulamaya devam ettikçe, insanlar sosyal medyaya ve çevrimiçi bilgilere erişmek için giderek daha fazla VPN'lere yöneliyor.
Kişilerin interneti daha özgürce kullanmak veya internette gezinirken geride dijital bir ayak izi bırakmamak için bir önlem olarak VPN'e yöneldiğini biliyoruz.

VPN'ler ne gibi korumalar sunabilir?

- Cihazınız ile VPN çıkışı arasına ekstra bir şifreleme katmanı ekleyerek trafiğinizin içeriğini ve meta verilerini ve internet gezintinizin gerçek hedefini internet servis sağlayıcınızdan (İSS) gizler.
- Trafiğinizi üçüncü bir ülke üzerinden yönlendirerek cihazınızın IP adresini web sitelerinden ve uygulamalardan gizler, bu da ülke tabanlı engelleri aşabilir.

Ne sunmuyorlar?

- Telefonunuzun varlığını IMSI yakalayıcılardan gizlemez.
- Cihazı fiziksel olarak kontrol eden birine karşı koruma sağlamaz, yani arama ve tarama geçmişi ve mesajlar da dahil olmak üzere cihazdaki içeriği gizlemez.
- GPS veya baz istasyonu üçgenlemesinden elde edilen cihazın fiziksel konumunu gizlemez, yani konumunuzu gizlemek için başka önlemler almadıysanız, örneğin sosyal medyadaki paylaşımlarınızı konum olarak etiketlemediyseniz sizi korumaz.

VPN nedir?

VPN, Sanal Özel Ağ, internet trafiğinizi bir veya daha fazla sunucu üzerinden yönlendirerek daha geniş internete erişmesini sağlar.
VPN'ler genellikle iş bağlamlarında fiziksel olarak ofis dışında bulunan kişileri dahili hizmetlere bağlamak veya coğrafi olarak ayrı siteleri bir intranete bağlamak için kullanılır. Ticari VPN'ler, sosyal medya ve iletişim platformlarına erişimin engellendiği ülkelerde giderek daha popüler hale gelmektedir, çünkü VPN sunucusu engelleyen ülkenin dışında bulunuyorsa bu web sitelerine erişim sağlar. Bu ticari VPN sunucuları genellikle başka ülkelerde, hatta başka kıtalarda bulunur. Sonuç olarak, web sitelerini fiziksel olarak VPN sunucusu ülkesindeymişsiniz gibi ziyaret etmenize izin verirler.

Günümüzde dünyada hükümetler ve/veya kötü niyetli kişi ve kurumlar web sitelerini insanların çevrimiçi faaliyetlerini gözetlemek, engellemek de dahil olmak üzere Web'e erişim üzerinde kontrol uygulamaya devam ettikçe, insanlar sosyal medyaya ve çevrimiçi bilgilere erişmek için giderek daha fazla VPN'lere yöneliyor. Kişilerin interneti daha özgürce kullanmak veya internette gezinirken geride dijital bir ayak izi bırakmamak için bir önlem olarak VPN'e yöneldiğini biliyoruz.

VPN'ler ne gibi korumalar sunabilir?

- VPN, cihazınız ile VPN çıkışı arasına ekstra bir şifreleme katmanı ekleyerek trafiğinizin içeriğini ve meta verilerini ve internette gezinmenizin gerçek hedefini internet servis sağlayıcınızdan (İSS) gizleyebilir.
- Trafiğinizi üçüncü bir ülke üzerinden yönlendirerek cihazınızın IP adresini web sitelerinden ve uygulamalardan gizler, bu da ülke tabanlı engelleri aşabilir.

Ne sunmuyorlar?

- Telefonunuzun varlığını IMSI yakalayıcılardan gizlemez.
- Cihazın fiziksel kontrolüne sahip birine karşı koruma sağlamaz, yani arama; tarama geçmişi ve mesajlar dahil olmak üzere cihazın kendisindeki içeriği gizlemez.
- GPS veya baz istasyonu üçgenlemesinden elde edilen cihazın fiziksel konumunu gizlemez, yani konumunuzu gizlemek için başka önlemler almadıysanız, örneğin Sosyal Medyadaki paylaşımlarınızı coğrafi olarak etiketlemediyseniz sizi korumaz.

VPN'lerin koruma sınırları

- Ticari ve ücretsiz VPN'ler "gizlilik" ve "güvenlik" hakkında birçok iddiada bulunur, ancak sundukları şeylerin sınırları vardır.
- Gerçekte, telefon şirketiniz, İSS'niz veya WiFi hizmetinizden VPN sağlayıcısına kadar İnternet trafiğinizin gerçek kaynağını ve hedefini görmek için kime güvendiğinizi değiştiriyorsunuz.
- VPN trafiği bir noktada bir sunucudan internete erişmek zorundadır ve bu sunucular ulus devletler ve diğer kötü niyetli aktörler tarafından gözlemlenmeye hazırdır.
- Tüm teknolojiler gibi VPN'ler de hata yapabilir. Bu, trafiğin yönlendirilmemesi veya yeterince motive olmuş bir saldırgan tarafından tespit edilmenize izin verebilecek belirli trafik türlerinin yönlendirilmemesi anlamına gelebilir. Bu hatanın farkında olmayabilirsiniz, yani her zamanki İSS'niz aracılığıyla yanlışlıkla sosyal medyada paylaşım yapabilir veya gerçek IP adresinizi kullanarak bir web sitesini ziyaret edebilirsiniz.

VPN seçerken nelere dikkat etmelisiniz?

- Bir VPN seçerken, VPN sağlayıcısının yetki alanına dikkat etmek önemlidir. Güçlü veri koruma ve gizlilik yasalarının yürürlükte olduğu ülkelerde bulunan VPN'leri aramayı düşünün.
- VPN sizden ne talep ediyor- özellikle de ücretsizse. Bazı VPN'ler, başkalarının cihazınızı tünellerinin çıkışı olarak kullanmasına izin verir, yani trafikleri sizin cihazınızdan geliyor gibi görünecektir. Örneğin, başka bir kullanıcı yasa dışı faaliyetlerde bulunursa bu sizin için sorun yaratabilir.
- VPN'i seçerken, internet trafiğinizin gerçek kaynağını ve hedefini görmek için güvendiğiniz kişiyi, telefon şirketinizden, internet servis sağlayıcınızdan veya WiFi hizmetinden VPN sağlayıcısına değiştirdiğinizi unutmayın. Diğer birçok teknoloji çözümünde olduğu gibi VPN de hatasız değildir. Örneğin, VPN trafiği bir noktada bir sunucudan internete erişmek zorundadır ve bu sunucular ulus devletler ve diğer kötü niyetli aktörler tarafından gözlemlenmeye hazırdır. Benzer şekilde, tüm teknolojiler gibi VPN'ler de hata yapabilir. Bu, trafiğin yönlendirilmemesi veya belirli trafik türlerinin yönlendirilmemesi anlamına gelebilir, bu da yeterince motive olmuş bir saldırgan tarafından- bazen sizin bilginiz olmadan- tanımlanmanıza izin verebilir.
- Atabileceğiniz başka adımlar da vardır, ancak hiçbiri mükemmel çözümler değildir.

Privacy International

62 Britton Street London EC1M 5UY United Kingdom

+44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).