



PRATİK DİJİTAL GÜVENLİK

Riskli Çevrelerde Pratik
Sibergüvenlik için bir Kılavuz



MICROSOFT
WINDOWS



PRATİK DİJİTAL GÜVENLİK

practicaldigitalprotection.com



Copyright 2017

CC BY-NC 4.0

Creative Commons Attribution-NonCommercial 4.0 International License

İÇİNDEKİLER ÖNSÖZ GİRİŞ

■ BÖLÜM 1: RİSKLER	8
ALT BÖLÜM 1: Karşı Karşıya Kalabileceğiniz Tehditleri Tanıyın	9
Ek: Asgari Güvenliğe Dair	15
ALT BÖLÜM 2: Bilgisayarınızı Hazırlamak	19
■ BÖLÜM 2: BİLGİSAYAR GÜVENLİĞİ	26
ALT BÖLÜM 3: Temel Kurallar	27
ALT BÖLÜM 4: Bilgiyi Edinme	31
Teknik Çözüm: Firefox ve Uzantılar	38
Teknik Çözüm: TOR	42
ALT BÖLÜM 5: Bilgiyi Depolama	45
Teknik Çözüm: Temel Şifreleme	50
Teknik Çözüm: Gelişmiş Şifreleme	53
ALT BÖLÜM 6: Bilgiyi Paylaşma	60
Teknik Çözüm: Proton Mail	68
Ek: Metadata	71
ALT BÖLÜM 7: Bilgiyi Silme	75
Teknik Çözüm: CCleaner	81
■ BÖLÜM 3: TELEFON GÜVENLİĞİ	84
ALT BÖLÜM 8: Telefon Güvenliği	85
ALT BÖLÜM 9: Telefonunuzu Kullanma	89
ALT BÖLÜM 10: Telefonunuzu Hazırlama	95
Ek: Konum Takibi	101
ALT BÖLÜM 11: Kullanılabilir Güvenli Uygulamalar	102
■ BÖLÜM 4: ENGELLEYİCİ GÜVENLİK	108
ALT BÖLÜM 12: Engelleyici Koruma	109

ÖNSÖZ

Eğer bu satırları okuyorsanız, şu veya bu şekilde temel siber güvenlik tehditlerine dair bir fikriniz olduğunu düşünüyoruz. Bu kılavuz size kilit siber güvenlik sorunlarını ve bunları engellemek için nasıl adımlar atabileceğinizi göstermek amacıyla tasarlandı. Bu kılavuzun çok temel bir hedefi bulunmaktadır. Siber güvenliğe dair yaklaşımınız günümüzde büyük bir önem arz etmekte: Bu yaklaşım sizin, dostlarınızın, kaynaklarınızın veya meslektaşlarınızın özgürlüğünü artık birinci derecede tayin eder haldedir. Haliyle bu kılavuz teknik bir siber güvenlik kitapçığından ziyade, dijital dünyada daha emniyetli davranmaya yöneliktir.

Bu kılavuzun biri gazeteciler, avukatlar, STK çalışanları, aktivistler için siber güvenlikle ilgili gerçek ihtiyaçlara karşılık gelmek ve onlara kaynaklık etmektir.

“Karşılaştığınız bir çok tehdit, dijital tehditlerden ziyade fiziksel tehditler.”

Bir Edward Snowden'ı duymuş, NSA'yi, ABD'yi ve Birleşik Krallık'ı ifşa eden işlerinden bir şekilde haberdar olmuşuzdur. Bir çok Amerikan filminde elektronik gözetleme sistemlerini görmüş veya devlet ajanlarının ve özel 'hacker'ların şifreler kırarak veri çalışını izlemiştir. Fakat bunların çoğu dünyanın birçok yerinde çalışan insan hakları savunucuları için ne yazık ki hiçbir şey ifade etmiyor. Gerçek tehdit güçlü devletlerin, dev şirketlerin veya özel olarak tutulmuş hackerların sizin bilgilerinize ulaşmasında değil; gerçek tehdit alıkonulduğunuz, gözaltına alındığınız bir durumda bilgisayarınıza, telefonunuza veya herhangi bir elektronik cihazınıza el konulduğunda ne yaptığınızın altında yatmaktadır. İşte tam bu noktadan hareketle kılavuz, dijital güvenliğe dair daha davranışsal bir yaklaşımı odağına almaya çalışacaktır.

Siber güvenlik anlamında faaliyet göstermeye dair karşılaşılan riskler ve tehditler, dünyanın bir çok ülkesindeki durumdan fazlasıyla farklı. Karşılaştığınız bir çok tehdit dijital tehditlerden ziyade, fiziksel tehditler. Bu kılavuz geniş bir yelpazedeki gazeteciler, STK çalışanları ve bulunan bir çok kişinin katılımı ve fikirleriyle geliştirilmiş ve en yaygın risklere karşı hareket etmek ve önlem alabilmek adına bir rehber niteliğinde basılmıştır.

Geçmişte katılmış olduğunuz bu konudaki bazı eğitimler çoğunlukla çeşitli teknik çözümlerin bir derlemesi olup, bir çoğu gereksiz ölçüde gelişmiş olabilir. Bu gibi eğitimlerin bahsettiğimiz eksikliği çoğunlukla katılımcı bir tartışmanın eksikliğinden kaynaklanmaktadır; davranışlarımızdaki ve yaklaşımımızdaki ufak

değişiklikler çoğu zaman gelişmiş teknik çözümlere nazaran çok daha faydalı sonuçlar doğurmaktadır. Kılavuz, bu fikri belleğinde tutarak cevaplar üreten niteliktedir.

Son olarak sibergüvenlik üzerine bir kılavuz üretirken insanlar tarafından deneyimlenmiş gerçek öyküleri, davranışsal örüntüleri ve sınırlamaları eklememek, büyük bir zaman kaybı olurdu. Bazen bu konudaki eğitimler ve kaynak niteliğindeki belgeler, günlük hayatınızdaki kullanım ve verimlilik konularını es geçip hızla en sofistike çözümlere atlayabilmektedir. Bu da çoğunlukla öğrenilen yöntemlerin kişilerce bir süre boyunca kullanılıp ardından terk edilmesine, böylece işin amacına ulaşamamasına neden olmaktadır. Gerçekten faydalı olma fikrini taşıyan bir kılavuz, bir orta yol bulmak durumundadır.

Bu kılavuz yukarıda adını geçirdiğimiz meseleler üzerine yoğunlaşacaktır ve muhtemelen karşılaştığınız güvenlik risklerini adım adım tanıtmaya ve tanımlamaya çalışan, kendi kendinize veya çeşitli eğitimlerde kullanabileceğiniz bir kaynak, bir rehber olarak tasarlanmıştır.

GİRİŞ

Sibergüvenlik üzerine kendi kendinize çalışabileceğiniz bu pratik kılavuza hoşgeldiniz. Neredeyse bir gün gibi kısa bir sürede bu kılavuz size güvenliğinize tehdit oluşturan riskleri anlamanızda yardım edecek ve bilgisayar/telefon kullanımınızla ilgili güvenlik seviyenizi belirgin ölçüde arttırmanızı sağlayacaktır.

Kılavuzun takibini kolaylaştırması açısından okuma sırasında lütfen dizüstü bilgisayarınızı ve telefonunuzu yanınızda bulundurunuz.

Kılavuzun okunulabilirliğini arttırmak için çoğu bölüm birbirine benzer yapıdadır. Çoğu bölüm genel bir tanıtımla başlayıp, bölüm içerisindeki kavramların anlatımıyla devam etmektedir. Bunun ardından bölümler, bahsi geçen riskleri sınırlandırmak için çeşitli davranışsal değişiklikler önerir ve teknik çözümlerle sonuca bağlanır. Bu teknik çözümler çoğunlukla ekran görüntüleriyle anlatılmaktadır.

Bölümler arasında bazı hikayeler bulunmaktadır. Bu hikayeler gerçek vakalara dayanmaktadır ve önerilen çözümlerin kullanılmasının (veya kullanılmamasının) doğrudan etkilerini anlatmaktadır. Bu vakalar çeşitli STK çalışanlarına, aktivistlere, muhabirlere, gazetecilere ve avukatlara aittir, fakat hikayeler anonim veya takma isimlerle sunulmaktadır.

Bu kılavuz dört bölüme ve oniki alt bölüme ayrılmıştır.

Birinci Bölüm karşınızdaki olan riskleri anlamaya odaklanır. Kendi durumunuzu analiz etmenize yarayacak araçları size sunmak için tasarlanmıştır. Ayrıca başlamadan önce bilgisayarınızda yapmanız gereken bir kaç değişikliği de içermektedir.

İkinci Bölüm hard disk şifreleme, güvenli tarayıcı kullanımı veya silme gibi önemli başlıkları kendi alt bölümlerinde açmaktadır. Bu alt bölümleri hem davranışsal hem de teknik değişiklikler ve öneriler izler, ardından gerektiği yerde bu değişikliklerin yapılışı adım adım gösterilir.

Üçüncü Bölüm telefon odaklı güvenlik meselelerini kapsar. Bilgisayarlara uygulanabilen çoğu şey genellikle telefonlara uygulanabilir olsa da bu bölüm daha çok telefonlarla ilgili tehditlere ve çözümlere odaklanır.

Dördüncü bölüm engelleyici güvenliği kapsar. Güvenliğinizi garanti altına almak için sibergüvenlikle ilgili olmayan, daha pratik ve davranışsal eylemlerle kendinizi nasıl koruyabileceğinizi; bir başka deyişle “en kötüsüne nasıl hazırlanacağınızı” anlatmaktadır.

BÖLÜM 1 RİSKLER



ALT BÖLÜM 1

KARŞI KARŞIYA KALABİLECEĞİNİZ TEHDİTLERİ TANIYIN



Bu bölümü okuyarak dijital güvenlikle ilgili ve karşı karşıya kalabileceğiniz çeşitli tehditlere dair fikir edineceksiniz. Bu temel kuralları bilmek kılavuzun devamını daha iyi anlamınıza ve kullanmanıza yarayacaktır.

Karşı karşıya kalabileceğiniz tehditleri anlamazsanız, kendinizi korumak için attığınız adımlar çok da büyük olmayacaktır. Bu durumda kendinizi hem çevrimiçi hem çevrimdışı durumlarda ihtiyacınız olmayan korunma yöntemlerini kullanırken veya güvenliğe dair anahtar adımları atarken bulabilirsiniz. Bu bölüm en yaygın tehditleri kısaca taslaklandırmaya çalışıyor. Burada gördüğünüz tehdit tiplerinden biri sizi doğrudan etkiliyor ve ilgilendiriyorsa, internetten bilgi almaktan veya uzmanlara danışmaktan çekinmeyin. Bölümün sonunda kaynakları görebilirsiniz. İyi kaynaklar bulmakta zorlanıyorsanız, meseleler çok teknik veya yeterince açık değilse, destek için bizle iletişime geçebilirsiniz.

DEVRE DIŞI BIRAKMAYA ZORLANMAK

Bu durum, kılavuzun basımında başat rol oynuyor. Zira Türkiye’de çalışanların dijital güvenliğine dair yüksek seviyede hacklenmeden daha çetin tehditler var. Buradaki ana tehdit, başkaları tarafından baskı yoluyla kendi güvenliğinizi devre dışı bırakmaya zorlanmaktır. (e-mail şifrelerinizin zorla edinilmesi, şifrelenmiş belleklerinize erişilmesi gibi) Kılavuz verilen örnekler ışığında kendine tam da bu meseleyi dert edindi ve bahsi geçen durumlarda kişiye rehberlik etmek amacını taşıyor. Unutulmaması gereken bu gibi tehditleri alt etmenin tek yolunun teknolojik önlemlerden değil, davranışlarımızdan ve alışkanlıklarımızda yapacağımız değişikliklerden de geçebildiği.

ARKA KAPIDAN MÜSAADE ETMEK

Aylık maaşınızın tamamını yeni ve sağlam bir kapıya harcadığınızda, kilit almayı unutmazsınız değil mi? Ya da kapınızın sağlamlığına güvenip, birinci katta oturmanıza rağmen demirliksiz açık bırakmazsınız. Ne yazık ki iş dijital güvenliğe geldiğinde birçok insan bunu yapabiliyor. Çok uzun ve güçlü şifreler kullanıp, internet tarayıcınızın geçmişini temiz tutsanız da, akıllı telefonunuza yükleyeceğiniz küçük bir uygulama korumaya çalıştığınız tüm verilerinizi erişilebilir hale getirebilir. Üstelik bir şifreye ihtiyaç bile duymadan! Veya tersine aynı uygulamaya telefonunuzun tarayıcısından girmeniz (ve tarayıcıda uygulamayı açık bırakmanız) telefonunuza fiziksel veya online olarak erişen herkesin bilgilerinize ulaşmasına neden olabilir. Bütüncül bir güvenlik kendi durumunuzu analiz etmenizi ve birbiriyle bağlantılı zaafları anlamanızı gerektiriyor.

Hizmetleri nasıl kullandığınızı görmek, bu hizmetlerin nasıl çalıştıklarını anlamak, bunlardan doğacak güvenlik zaafılarını ortadan kaldırmanızın en önemli ayağı.

ETME

Günümüzde akıllı telefonlar bilgisayarlara, bilgisayarlar da akıllı telefonlara benziyor. GPS, kablosuz bağlantılar ve radyo (telefon) sinyalleri gibi birçok bağlantı yolu, bilgisayarınızın veya akıllı telefonunuzun yerini takip etmeyi kolaylaştıran izler olabilirler. Takip ve izleme süreçlerinde kullanılan cihazların pahalı olmadığını eklersek, sürekli olarak herhangi birinin sizi kolaylıkla takip edebildiğini varsayın. Unutmayın: İçerisinde bir SIM kart olmasa dahi telefonunuz konum sinyalleri göndermeye devam eder. Uygulamalar yüklendiklerinde çoğunlukla konumunuza erişmek isterler; bu da üçüncü kişilerin size takip etmesi için bir başka kapı olabilir. Bu konuda daha fazla bilgi edinmek için Google'ı kullanabilir, yukarıdaki terimlerin İngilizcesi olan Localization ve Triangulation kavramlarını aratabilirsiniz.

ARAMALARIN, (CHATS), E-POSTALARIN YOLUNU KESMEK

SMS'lerinizi, e-postalarınızı, sohbet mesajlarınızı ve telefon aramalarınızı şifrelemediğiniz sürece yazdığınız her şey karşı tarafa 'düz metin' olarak ulaşır. Bu mesajlarınızı sadece hizmet sağlayıcınızın değil, ağınıza bağlı herkesin okuyabileceği anlamına gelir. Günümüzde kullanılan hizmetlerin çoğu bir biçimiyle şifreleme kullanıyor, fakat bunların bazıları bu sistemi sizin manuel olarak açmanızı gerektiriyor. E-postaları, telefon konuşmalarını ve mesajları paylaşmayı reddeden uygulamaların ve servislerin kimler olduğunu öğrenmek, yanı sıra hangi hizmetlerin hedef alındığını bilmek çok önemli. Bu uygulamaları, hizmetleri ve bunları sağlayan kurumları bilmek, kişisel iletişim bilgilerinizi üçüncü kişilerle paylaşmak konusunda anlaşmalar yapmış olan firmalardan kaçınmak, haberleşme güvenliğinizi sağlamadaki en büyük adım. Hatırlayın; temel problem e-posta veya mesaj göndermek değil, bu mesajlara elektronik aletlerinize el konup ulaşıldığında ve şifreleriniz zorla alındığında neler olduğu. (Bu bilgilere ayrıca oturum kimlik bilgileri de deniyor.)

Bilgisayarlar ve telefonlar için çoğu işletim sistemi (OS) kolay kullanıma uygun ayarlarla gelir. Güvenliğe uygun değil! Bu nedenle ilk adım olarak cihazlarınızın genel ayarlarını gözden geçirmeniz ve güvenliğinizi artırma yönünde gerekli değişiklikleri yapmanız gerekir.

KIRMA

Bir şifre dakikalar içinde kırılabilir. Elektronikte kullanılan Zorla Deneme yöntemini kullanarak (yani elektronik bir cihaz veya yazılımla dakikada milyonlarca şifre denemesi yaparak) 4-6 karakterli bir şifreyi çözmek bir saat içinde mümkündür. Özellikle güvenliğinizi için başat rolleri olan iş e-postaları veya şifrelenmiş bellek/depolama sistemleri için şifre seçerken bunu göz önünde bulundurun. Telefonunuzu tesadüfen sokakta bulmuş birini durdurmada kısa bir şifre iş görebilir, fakat aynı şifre sizi profesyonellerden koruyamaz. Parolalarınızı harfler, işaretler ve sayılar içeren, büyük küçük harf duyarlı ve uzun olanlarından seçmeye, dahası parolanızı sık sık değiştirmeye özen gösterin.

HACKLENME, KORSAN AMAÇLI PROGRAMLAR VE

Bu kılavuz ileri düzeydeki hack tehditlerine, zira bunun gazeteciler veya avukatların başına gelmesi çok olası. Yine de virüslerin ve korsan amaçlı programların (sizden gizlenen ve başkalarının bilgisayarınıza erişmesini sağlayan yazılımlar) yaygın tehditler olduğunu bilin ve bunların daha ziyade ekonomik suçlar veya kimlik hırsızlığında kullanıldığını aklınızda tutun. Yine de bu tehditlerden korunmanın, bütüncül bir güvenlik için bir parça olduğunu da ihmal etmeyin. Bilgisayarınızda 'güvenlik duvarı'nın aktif olduğunu,

arka planda virüs programlarının çalıştığını ve otomatik güncellemelerin açık olduğundan emin olun. Güncellemeler en yeni tehditlerin tespiti ve engellenmesini garanti altına alır. Güncelliğini yitirmiş anti-virüs programları güvenlik sağlamaz.

AĞLAR

Eğer herhangi bir kişi ya da kurum, size karşı bir dava açmak veya iletişimde olduğunuz birinin peşine düşmek için bilgilerinize gizlice ulaşmak istiyorsa, ağız (network) doğal bir saldırı alanına dönüşür. Bu özellikle herkese açık ve korunmasız wi-fi ağlarına sahip küçük organizasyonlar için daha büyük bir tehlikedir. Evinizde veya ofisinizde modeminizin sahip olduğu kullanıcı ismini veya şifreyi hiç değiştirdiniz mi? Çoğunlukla bu işlemi uzun süreler. Bir şekilde modeminize ulaşan biri ağıza ulaşmış, ağıza ulaşan biri de bilgisayarınıza ve verilerinize ulaşmış demektir. Kamusal wi-fi ağları da tehlikelere daha açıktır. Bu ağları kullandığınızda, yani kafelerde, kütüphanelerde, otellerde ve toplu taşıma araçlarında daha dikkatli olmalısınız.

DOSYA KURTARMA

Bir dosyayı sildiğinizde, geri dönüşüm kutunuzu boşalttığınızda, veya bir dosyayı bilgisayarınızdan USB ya da harici belleğe taşıdığınızda, aslında hiçbir şey silinmez. Hiçbir şey! Tüm dosyalarınız yerli yerinde durur ve uzun yıllar da durmaya devam edebilir. Bu dosyalara kısa zamanda ve çok az kabiliyetle erişilebilir. Geçmişte bilgisayarınızdan sildiğiniz tüm dosyaları bulmak ve görmek için ücretsiz indirilebilir programlar internette. Dosya silmeye dair kılavuzun bu bölümü belki de en önemli bölüm; zira bu kullanıcıların en zayıf olduğu alan.

Bu kavramları ve ne gibi sorunlar yaratabileceklerini anlayabildiniz mi? Eğer anlayamadıysanız, lütfen bir sonraki bölüme geçmeden önce anlamadığınız kısımlara dair araştırma yapın. Bu kısımda önem arz eden ve en sık karşılaşılan meseleler;, telefonunuzun (veya bilgisayarınızın) konumunun başkalarının sizi takip etmek için kullanılabildiği ve bunu nasıl durdurabileceğiniz ile dosya kurtarma ve silme işlemlerinin bilgisayarınız başkalarının eline geçtiğinde zayıf noktanız olacağı idi.

RİSKLERİNİZİ VE İHTİYAÇLARİNİZİ DEĞERLENDİRMEK

Bu kılavuzda ilerlemeden önce kılavuzun size ve karşılaştığınız durumlara nasıl uygulanabileceğini anlamanız gerek. Bu kılavuz boyunca anlatılan vaka çalışmaları ve hikayeler bir avukat, gazeteci veya STK çalışanı olarak ne gibi tehditlerle karşı karşıya olduğunuzu berrakça ifade etmeye çalışırken, aynı zamanda bu tehditleri ortadan kaldırmaya yönelik çözümlerin neler olduğunu ve bunların kolayca sağlanabilirliğini göstermeye uğraşiyor. Kişisel olarak işinizden ötürü zarar görmeye dair korkularınız olmasa dahi, takip edilebileceğinizi unutmayın. Eğer çalışma arkadaşlarınızın veya dostlarınızın başına bir şey gelirse, sorgulanmak üzere alkonabilirsiniz veya eşyalarınıza el konulabilir. Eğer hali hazırda gerekli adımları atmadıysanız veya iş arkadaşlarınız ya da dostlarınızla korunma stratejilerini tartışmadıysanız, bu durum siz ve çevrenizdekiler için yeni bir güvenlik meselesine dönüşebilir. Bir plan yapmak için çok geç olabilir.

“Güvenliği ciddiye almak, küçük sorunları küçük tutar.”

ADIM: KORUMANIZ GEREK?

Ne gibi bilgilerle çalışıyorsunuz? Bu bilgiler aleyhinize kullanılmak üzere ele geçirildiğinde sizi nasıl etkileyebilir? Daha da önemlisi, bunlar başkalarını nasıl etkileyebilir? Eğer hard diskinizin tamamı ele geçirilirse, üçüncü kişiler hakkınızda ve işinize dair neler öğrenebilir?

ADIM: ALTINDA?

Tek bir telefonunuz mu var? Belki bir verdiğiniz veya sattığınız bir başka telefonunuz olmuştur. Kendi kullanımınız için tek bir bilgisayara mı erişiminiz var, yoksa ofis hayatınızda bir başka bilgisayar daha mı kullanıyorsunuz? Dizüstü bilgisayarınızın veya tabletinizin kullanımını bazen arkadaşlarınızla, ev ahalisiyle veya aile bireylerinizle paylaşıyor musunuz? Belirli bir seviyeye ayarladığınız güvenlik ayarlarına sahip oturma odanızın, kullanımını paylaştığınız kişilerce veya bu kişilerin farklı oturma odasıyla sekteye uğratılma/uğrama ihtimali var mı? Cihazlarınızın her zaman sizin yanınızda mı bulunuyor yoksa başkalarının elinde, ofiste, bir kafede veya bir kütüphanede, hatta bir kafe çalışanının veya arkadaşınızın gözetiminde kalıyor mu? Kullandığınız veya yakın zamanda kullandığınız, potansiyel olarak hassas veriye sahip tüm cihazların bir listesini yapın. Cihazlarınızın sadece sizin kullanımınıza ait olmasıyla, başkalarıyla paylaştığınız bir kullanıma sahip olması arasında ciddi güvenlik farkları olabileceğini aklınızda tutun.

ÜÇÜNCÜ ADIM: NEDEN

Gazeteci misiniz? Hedef aslında siz değil de kaynaklarınız mı? Bir STK çalışanı mısınız? Faaliyetlerinizi haritalandırmak, kimlerle iletişim kurduğunuzu öğrenmek veya kimler tarafından fonlandığınızı öğrenmek mi istiyorlar? Belki de marjinal toplulukları veya örgütleri, bireyleri veya seks işçilerini destekleyen kuruluşlarla çalışıyorsunuz ve birlikte/adına çalıştığınız kişi ve kurumların kimliklerinin gizliliği bu işin en kritik parçası. Çalıştığınız kurumun desteklediği kişilerin, kurumların ve örgütlenmelerin isimlerine ve kimliklerine ulaşmak adına hedef haline gelmeniz mümkün mü? Göçmenlere, ya da aktivistlere yasal destek sağlayan bir avukat mısınız? Büyük ölçekli hassas veriye veya röportajlara sahip bir araştırmacı ya da arşivci misiniz? Sahip olduğunuz verilere erişmek adına peşinize düşülmesi muhtemel mi?

DÖRDÜNCÜ ADIM

Güvenlik politikanıza karar vermede size kimin tehdit oluşturduğunu belirlemek en temel işlerden biri. Belki de hedef siz değilsiniz, fakat hedef gösterilen bir gazetede çalışıyorsunuz. Eğer böyleyse kim? Aktif bir hedef olmasanız da gelecekte bir hedefe nasıl dönüşebilirsiniz?

Bu soruların çoğu 12. bölümde “Engelleyici Koruma” başlığı altında derinlemesine cevaplandırılmaya çalışıldı. Şimdiden bu başlıklar üzerine kafa yormak bu kılavuzu daha anlamlı kılacak ve farklı bölümlerin size neden ve nasıl uygun olduğunu anlamanızı kolaylaştıracak. İşe riskleri değerlendirerek başlamaktaki sebep, hangi dijital güvenlik araçlarının uygun olduğuna karar vermenize yardımcı olacak olması. Kendinizi korumak için hangi davranışsal değişimler kullanışlı? Hangileri kılmayla alakalı? Bir kişi için işe yarayan bir yöntem bazen bir başkası için tamamen işlevsizdir. Hatta aynı anda ihtiyacınızdan çok daha fazla aracı ve taktiği uygulamanız üzerinizdeki tehdidi azaltmak bir yana, artırabilir bile.

EK: ASGARİ GÜVENLİĞE DAİR

3. kişilerce alıkonulduğunuzda veya bilgilerinize erişildiğinde, kendinizi koruyabileceğiniz alan fazlasıyla daralmış olur. Buna dair geliştirebileceğiniz en önemli önlem, kendinizi korumaya yönelik adımları önceden atmış olmanızdır. Bunu başarmanın kolay yolları mevcuttur ve bu adımları atmanız sizin, iş arkadaşlarınızın, sevdiklerinizi güvende veya risk altında olmaları arasındaki ince çizgidir.

3. kişiler bilgilerinize ulaşmak için gerektiğinde çok etkin biçimde, birbirinden farklı yöntemleri kullanabilirler. Bunu gerçekleştirecekleri bir sürü hizmet, e-posta ve başka çevrimiçi sistemler bulunmaktadır. Eğer herhangi bir zorla sizden bağlantı bilgilerinizi veya şifrelerinizi almaya çalışacaklarsa, çoğu zaman neyi sormaları gerektiğini bilmelidirler. 3. Ve yerel olarak çeşitli varsayımlar geliştirebilirler; bir bölgede Facebook hesabınızın olduğu varsayımı yapılırken, başka bir bölgede WeChat kullandığınızdan şüphelenebilirler. Fakat hali hazırda yaygın biçimde kullanılan bir kaç program ve hizmeti kenara koyarsak, nihayetinde size ne sormaları gerektiğini bulmaları icap edecektir.

Kılavuzun bu kısmında, buna dair en sık karşılaşılan durumlar, bu durumlar karşısında alınabilecek önlemler ve çözümler bulunmaktadır.

ÜÇÜNCÜ KİŞİLERCE VEYA UĞRAYABİLECEĞİNİZ ZARARI OLABİLDİĞİNCE SINIRLANDIRMAK

Öncelikle hesaplarınızın varlığı, başka kişilerin başına gelenlerden ötürü biliniyor olabilir. İrtibat halinde olduğunuz ortaklarınız, iş arkadaşlarınız veya kaynaklarınız üzerinden hesaplarınızın varlığından haberdar olunmuş, hatta bu hesaplarınızın içeriğine girilmiş bile olabilir. Bunun anlamı, önemli olanın hassas içerikli işleriniz için sadece ne söylemeniz veya bilgilerinizi nasıl depoladığınız değil; bu işler/ bilgiler için kategorize edilmiş e-posta veya sohbet hesapları oluşturmuş olmanızdır. Bu hesaplar gündelik olarak kullandığınız e-posta veya hesaplar olmamalıdır.

Bu hesaplarda tam adınızı kullanmamalısınız. Aynı zamanda yazışmalarınıza kimliğinize dair detayları, konumunuzu veya başka iletişim bilgilerinizi (Örneğin, telefon numaranızı) eklemekten kaçınmalısınız. Bunu uygulamanız size karşılaştığınız duruma göre en azından bir miktar alan açabilir, çeşitli suçlamalar karşısında inkar şansınızı doğurabilir.

Bu mesele en büyük kaygılardan bir tanesidir. Aynı zamanda bu mesele üzerindeki kontrol kabiliyetiniz ne yazık ki çok düşüktür, zira durum ağırlıklı olarak başka 3. Bağlıdır.

Bu riski sınırlandırmanın en güvenli yolu, hassas içerikli işlerinizin çoğunda otomatik yoketme (auto-destruct) fonksiyonuna sahip e-postalar veya sohbet programları kullanmanızdır. Bu fonksiyon kayıtlarınızı veya e-postalarınızı, tarafınca onaylanan bir sürenin sonunda (örneğin bir saat, bir gün veya bir hafta...) otomatik olarak siler. Kullanıcıların kimlikleri ifşa olsa dahi bu fonksiyon, yazışmalarınızın ve bilgilerinizin içeriğine erişimi ortadan kaldıracaktır. Bu hem sizin hem de yazıştığınız kişilerin güvenliği için kullanışlı bir yöntemdir zira unuttuğunuz durumda dahi yazışmalarınızın düzenli olarak silinir ve bu yazışmaların yeniden ele geçirilmesi mümkün değildir.

Otomatik yoketme özellikle tam anlamıyla tanımadığınız veya bilgi teknolojileri konusunda çok sınırlı bilgiye sahip kişilerle iletişim kurmak için ideal ve kullanışlı bir özelliktir. Ayrıca kullanımı fazlasıyla kolaydır. Bu özellik, çeşitli sohbet programlarına da uygulanabilir.

BİLGİSAYARINIZDAKİ İZLER VE KANİT NİTELİĞİ OLAN BİLGİLERCE UĞRAYABİLECEĞİNİZ ZARAR

Kullandığınız elektronik araçlara el konulduğu bir durumda 3. Hızla bu araçlar üzerinde bir teknik analize başlayabilirler. Bu yöntemle kullandığınız hesaplara ulaşılabilir ve bunun ulaşılan hesaplara dair sizden daha fazla bilgi alınmaya çalışılabilir. Başarıya ulaştıkları durumda 3. Elde ettikleri bilgiyi size veya başkalarına karşı kullanabilir. Bu meselenin fazlasıyla üzerinde durmanız gerekmektedir. Zihninizde bilgilerinize ulaşımı fazlasıyla karmaşık süreçlermiş gibi canlandırmayın. Örneğin kullandığınız internet tarayıcısı, çeşitli bilgileri kayıt altına alıp depolamaktadır. Bunların en bariz tipleri tarayıcınızdaki bir e-posta sağlayıcısının yer işareti veya geçmişte ziyaret ettiğiniz websitelerini gösteren çerezlerdir. Ayrıca tercihleriniz dahilinde daha gelişmiş verileri, örneğin bağlantı bilgileriniz, şifreleriniz de tarayıcınızca kaydedilmiş olabilir.

Tarayıcınıza bu bilgileri silmesi yönünde bir talimat verebilirsiniz. Fakat bu durumda tarayıcınızı her açtığınızda sosyal medya hesaplarınızdan, alışveriş sitelerindeki bilgilerinize kadar tüm detaylarınızı tek tek yeniden girmeniz gerekecektir. Ayrıca yine tercih ettiğiniz durumda tarayıcınız, yer işaretlerini kaydetmeyecektir. Bu genel bilgisayar kullanımının verimliliğini düşürecektir. Aynı zamanda bu durumda bir şeyler gizlediğiniz izlenimini de uyandırabilir.

Bunun yerine ilk yapmanız gereken, iki tarayıcı kullandığınız bir strateji geliştirmektir. Bunlardan ilki gündelik sörf ve kişisel kullanımlarınız için, diğeryse daha hassas e-postalarınıza, hesaplarınıza ulaşmak için veya hassas nitelikte araştırmalarınızda kullanılmalıdır. Tariflediğimiz ikinci tarayıcınız kullanımınız boyunca oluşan her türlü izi otomatik olarak silmeye ayarlanmalıdır. Ayrıca bu tarayıcı içerisine, tarayıcınızın kendi silme sistemine destek olacak ek güvenlik uzantıları eklenmelidir. Böylelikle tarayıcınız internet geçmişinizin izleri daha bütünlüklü ve kesin olarak silebilir.

İŞLETİM SİSTEMİNDEKİ İZLER VE KANİT NİTELİĞİ OLAN BİLGİLER

Tıpkı tarayıcınız gibi işletim sisteminizde de yaptığınız her şeyde izler toplanır. Buna internet erişimi de dahildir. Ayrıca kullandığınız yazı programlarının (örneğin MS Word) geçmiş kullanımları veya düzenlemeleri, verilerinizin geçici kopyaları ve bilgisayarınıza kaydettiğiniz aşağı yukarı her şey de bu izlere dahildir. Bu tip bilgilere erişmek, tarayıcınızı kurcalamaya nazaran çok daha derin bir teknik bilgi gerektirir fakat unutmayın ki 3. Bu konuda uzman olabilir veya buna dair bir çok kaynaktan yararlanıyor olabilirler.

Bu sorunu aşmak için geçmiş izleri ve geçici verileri bilgisayarınızdan silen bir program kullanmanız gerekmektedir. Ne şanslısınız ki, bu programları kullanmak fazlasıyla kolay.

“SİLİNİMİŞ MALZEME”

Sıklıkla yanlış anlaşılan konseptlerden biri de bir şeyi bilgisayarınızdan “silmenin” ne anlama geldiğidir. Bir şeyi “sildiğinizde” veya geri dönüşüm kutunuzu boşalttığınızda aslında hiçbir şey silinmiş olmaz. Burada bilgisayarınız veya cep telefonunuz silinen öğeyi ‘uygun alan’ olarak işaretleyip, ileride yeni verilerin buraya yüklenebilmesini sağlar. Yani “silinen öğe” aslında olduğu gibi yerinde durur. Bazı durumlarda bu süre yılları bulabilir. Başka durumlardaysa “silinen” verinin sadece bir kısmı yeni dosyalarca kaplanıp, kalan kısmı hala yerinde duruyor olabilir.

Bu "silinen" verileri siz göremeseniz de, onlara ulaşamasanız da, bu işlemleri gerçekleştirebilen, kullanımı kolay ve ücretsiz programlar mevcuttur. Bu programlar bu gibi verileri saptayıp, geri getirip, tekrar açıp sanki hiç "silinmemişler" gibi onlar üzerinde işlem yapmanızı mümkün kılarlar. Bahsi geçen programların kullanımı gerçekten çok kolaydır; teknolojiyle hiç arası olmayan kişiler bile beş dakika içerisinde programa hakim olabilirler. Unutmayın: 3. Bu duruma çoğunlukla aşınadılar ve bu tekniği bilgisayarınızda, USB'nizde, telefonunuzda ve diğer elektronik cihazlarınızda kullanabilirler.

VERİNİZ

Buradaki anahtar mesele belgelerinizden videolarınıza, fotoğraflarınızdan müzik dosyalarınıza kadar USB'nizde, telefonunuzda, harici sabit diskinizde veya kendi bilgisayarınızda tuttuğunuz/ depoladığınız tüm dosyalardır. Bu gibi verileri gerçekten korumanın tek yolu, veriyi fazlasıyla güvenli bir yerde tutmaktır. Bu "güvenli yer" de şifreli, bulunması güç bir sürücü/sabit disk olmalıdır.

Fakat bu şifrelemenin kendisi, bilgilerinizin ifşa olduğu veya teknik malzemelerinize el konulduğu durumlarda Bu şifreyi kırmaya ihtiyaç duymasıyla sonuçlanabilir. Bu nedenle bu gibi verilerinizi gerçekten korumanın yolu "gizli" şifreleme kullanmanızdır; böylelikle kimse sizin bilgilerinizi şifrelediğinizi göremeyecektir bile. Var olduğunu bilmedikleri verileri kimse sizden talep edemeyecektir.

İnanın bu gibi şifreleme programlarını kullanmak da anlattığımızdan kolaydır

Ayrıca herşeyi basitleştirmelisiniz. Bir alanda işinizle alakalı tüm belgeleri değil, sadece gerçekten ihtiyaç duyduklarınızı depolamalısınız. İş dosyalarınıza şu anda kabaca bir bakacak olduğunuzda, bu belgelerin çoğuna artık ihtiyaç duymadığınızı fark edeceksinizdir. Taslaklar, bir belgenin önceki/ ilkel sürümleri, ana dosyalara sonradan eklenen ufak parçalar vb. tüm veriler ihtiyacınız dışındaysa silinmelidir. Sadece ihtiyaç duyduğunuz şeyleri depolamaya özen gösterin.

Eğer elinizde kullanmayacağınız fakat arşivlemek istediğiniz eski dosyalar varsa, bunları güvenli bir bulut (cloud) deposuna aktarabilirsiniz. Bu gibi bir güvenli olmalıdır ve tercihen yaşadığınız ülkede sunuculara (server) sahip olmaması gerekmektedir. Ayrıca biraz önce bahsettiğimiz tarayıcınızla ilgili güvenlik önlemlerini, kullandığınız bulut için de düşünmelisiniz. Tarayıcınız üzerinden kimse bulut deponuza kolaylıkla ulaşmamalıdır.

TELEFONLAR, PAD'LER VE UYGULAMALAR

İş amaçlı kullanımlarınızı bilgisayarınız ve telefonunuz arasında ayırmalısınız. Bu kullanımlar düşmemeli ve birbiriyle çakışmamalıdır. Buraya kadar uyguladığınız tüm güvenlik yöntemleri, telefonunuzu dikkatsizce kullanmanızdan ötürü boşa gidebilir. Otomatik yoketme özellikli e-postaların, temiz tuttuğunuz bir tarayıcının, aynı bilgilere telefonunuz üzerinden ulaşılabilirdiği durumda ne gibi bir faydası olabilir?

Herkes hesaplarına ve kullandığı hizmetlere ulaşmak için telefonlarında uygulamalar kullanmaktadır. Mobil uygulamalar kullanıyor olmak 3. Kişilere (sınırlı da olsa) hesaplarınıza erişim sağlayabilir (örneğin e-postalarınız). Ayrıca bu uygulamaları şifreli kullanıyor olsanız, hangisini kullanıyor olduğunuza dair başkalarına fikir verir. Kısaca telefonunuz, bilgisayarınızda bütün güvenlik önlemlerini boşa düşürebilir. Telefonunuzu nasıl kullanacağınıza dair net bir tavır benimseyin ve ne

gibi programları/ hizmetleri kullandığınıza dair başkalarına fikir verecek uygulamaları kullanmaktan mümkün mertebe kaçınin. Genellikle mobil uygulamalarınızı indirirken veya ayarlarken, bu uygulamaların konumunuza, kameranıza veya rehberinize erişmesine izin vermeniz gerekir. Dahası, telefonunuzdaki tarayıcıları hassas e-postalarınız için sakın kullanmayın, zira telefonda depolanan izleri silmek neredeyse mümkün değildir. Ayrıca telefondaki bir bilgiyi gerçek anlamda silmek çok daha güçtür. Bu nedenle telefonunuzda işinizle ilgili hassas bilgileri asla depolamamalı veya sonradan bilgisayarınıza aktarmak üzere telefonunuza bu gibi bilgileri indirmemelisiniz.

siz

Son olarak, Siz. Siz hem kendinize, hem de başkalarına karşı en büyük tehdidi oluşturmaktasınız. Bilgilerinizi ve verilerinizi korumak, önden planlamayı gerektirmektedir. Risk analizi yapmanın haricinde, çeşitli nedenlerle alıkonulduğunuz durumlarda nasıl davranacağınızı planlamalı ve bu planı güvendiğiniz birkaç kişiyle paylaşmalısınız. Hangi bilgileri paylaşmanız sakınca atfetmezken (bazı durumlarda bir şeyler paylaşmanız, hiçbir şey paylaşmamaktan daha iyidir zira hiçbir şey paylaşmamak, bir şeyler sakladığınız duygusunu pekiştirebilir), hangi bilgileri korumanız zorunludur? Aynı şekilde, başka ortaklarla çalışıyorsanız, herkesle beraber bir stratejiyi tartışmalı ve bu konuda çeşitli mutabakatlara varmalısınız.

Politika dünyasında kullanılan bir tabir vardır: Halkın her halükarda öğreneceği bir şey hakkında asla yalan söyleme. Siz'in için bu, başkalarının zaten erişebileceği bilgiler hakkında yalan söylememeniz anlamına gelmektedir. Bu konuda teknik bir çözüm ne yazık ki yoktur; buradan sonrası önceden aldığınız önlemlere ve zekanızın kıvraklığına bağlıdır.

FAKAT

Bu günlerde bazı ülkelerde kimlik bilgilerinizi paylaşmadan bir SIM kart edinmek pek mümkün değildir. Ayrıca herhangi bir İnternet Hizmet Sağlayıcı'sından (ISP) internet erişimi talep ettiğinizde de kimlik bilgilerinizi gerekmektedir. Yine bazı ülkelerde telefon veya internet hizmeti sağlayan şirketler, bilgilerinizi üçüncü kişilerle paylaşıyor, bunlar hakkında herhangi bir yasal yaptırım da bulunmuyor olabilir. Ayrıca çoğunlukla bu şirketler, kullanıcıları hakkındaki bilgileri arşivlemek zorundadırlar. Bu bilgilere telefon kayıtlarınız, internet kullanımınız ve bu hizmetleri kullandığınız konumlar da dahildir.

Tüm bunların anlamı buraya kadar güvenliğinizi için attığınız tüm adımların bir seferde boşa düşürülebilir olmasıdır. Şanslısınız ki VPN veya TOR kullanarak internet sağlayıcınızdan bu gibi bilgilerin çok büyük bir kısmını saklayabilirsiniz. Bunu telefon sağlayıcılarına karşı uygulamak biraz daha güçtür, bu nedenle işiniz için bilgisayarınızı, telefonunuzdan daha çok kullanmanızı öneriyoruz.

ALT BÖLÜM 2

BİLGİSAYARINIZI

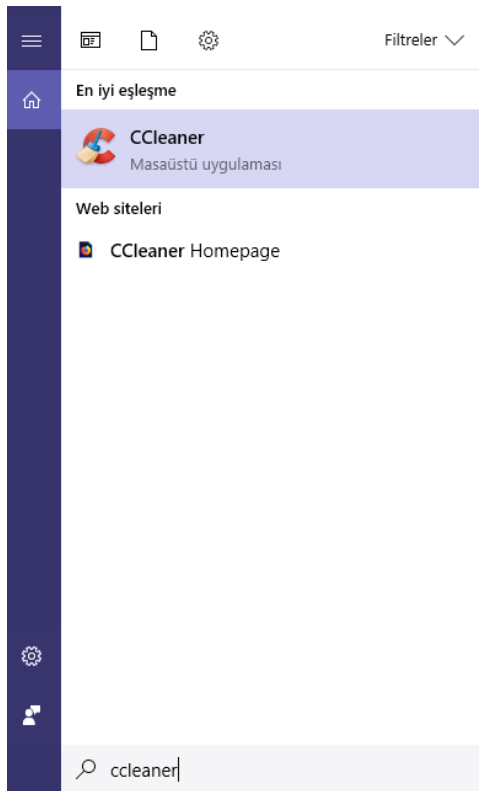
HAZIRLAMAK



Bu bölümbilgisayarınız için gözetmeniz gereken bazı ayarları göstermektedir. Bu bölüm aracılığıyla bilgisayarınızın temel ayarları hakkında daha derin bir bilgiye sahip olacak, hangi ayarları ne şekilde değiştirip kontrol edebileceğinizi öğrenebileceksiniz.

Kılavuzun geri kalanında teknik bilgiler için arama fonksiyonlarını kullanacağız. Teknik değişikliklerin yapılması gerektiğinde, spesifik bir ayarı bulmak için bir arama terimi kullanacağız. Bu arama fonksiyonlarına muhtemelen aşinasınızdır, fakat yine de emin olmak için, aşağıda arama bölgesinin yerini gösteren bir ekran görüntüsünü görebilirsiniz (O1).

Bu arama terimleri, bilgisayarınızda ikisini de kullanma ihtimalinizi gözeterek hem Türkçe, hem de İngilizce verilecektir.



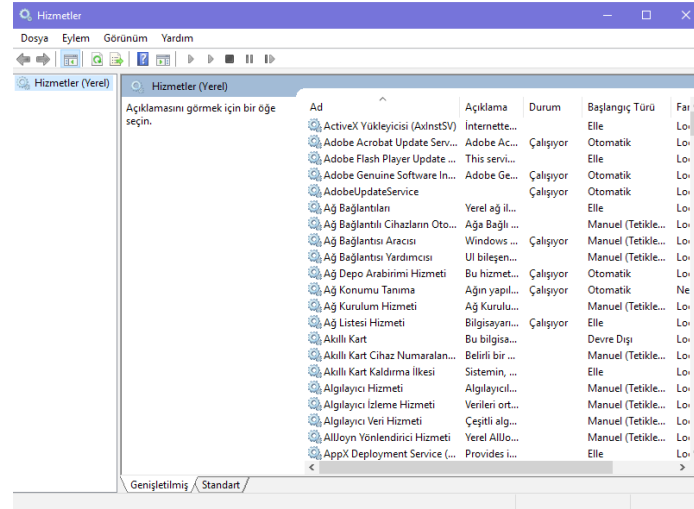
Win10 için, kılavuzun temel kısmına başlamadan önce gözden gereken meseleler üç bölüme ayrılmıştır; Hizmetler, Yerel Güvenlik İlkesi, ve Ayarlar.

Not: Eğer Windows'un eski sürümlerinden birini kullanıyorsanız, bu ayarların bir kısmı mevcut olmayabilir. Önerimiz, elinizdeki Windows sürümünü (bilgisayarınızın bu sürümle olduğu takdirde) Win10'a yükseltmenizdir. Daha yakın tarihli sürümlere dair yapılan güncellemeler, size daha iyi güvenlik seçenekleri sunacaktır.

Hizmetler bilgisayarınızın arka planında çalışırlar ve bir bilgisayarın neler yapabileceğine karar verirler. Örneğin bilgisayarınıza uzaktan erişimi engellemek için, uzaktan erişimi mümkün kılan hizmet devre dışı bırakılmalıdır (kapatılmalıdır). Güvenliğinizi arttırmak için kapatmanız gereken (devre dışı bırakmak) anahtar hizmetlerin bazılarını burada tanımlayacağız.

O1

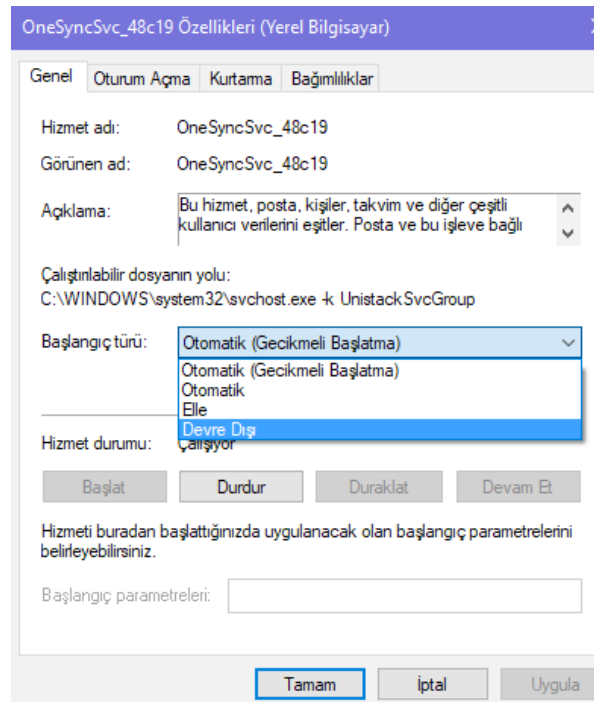
Win10 için, arama çubuğuna Hizmetler yazarak hizmetler penceresini açın. Açılacak ilk pencerede (02) listeyi takip ederek aşağıda listelenmiş hizmetleri bulun ve her birine çift tıklayın.



02

- Remote Desktop Configuration / Uzak Masaüstü Ayarları
- Remote Desktop services / Uzak Masaüstü hizmetleri
- Remote Registry / Uzak Kayıt Defteri
- Routing and Remote Access / Yönlendirme ve Uzaktan Erişim
- UPnP Device host / UPnP Aygıt Ana Makinesi
- Volume Shadow Copy (VSS) / Birim Gölge Kopyası
- File History Service / Dosya Geçmişi Hizmeti

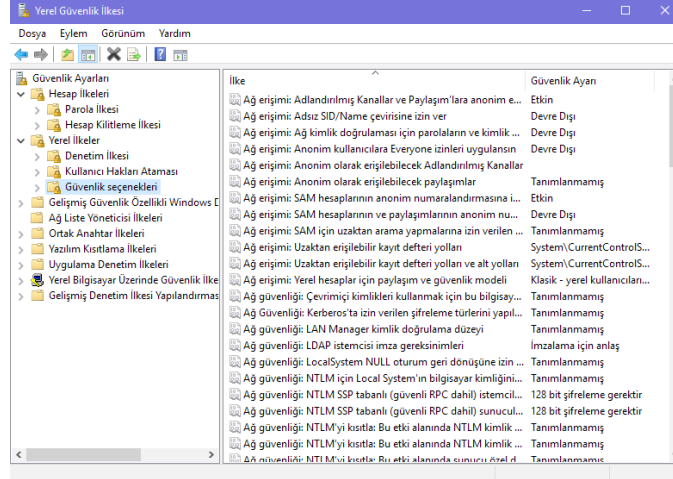
Açılan küçük pencerede (03), Başlangıç Türü'nü bulun, bunu Devre Dışı olarak değiştirin ve Tamam veya Uygula'ya tıklayın.



03

GÜVENLİK İLKESİ (YEREL)

Güvenlik ilkesi bölümü, güvenlikle ilgili meseleler için bir ilke belirlemenizi mümkün kılar. Örneğin işletim sisteminizi açmaya çalışan biri şifrenizi 5 kez yanlış girerse, bilgisayarınızın 1 saat boyunca donmasını sağlayabilirsiniz. Değiştirmeyi düşünmeniz gereken bazı güvenlik ilkeleri aşağıda sunulmuştur. Arama çubuğunuza Yerel Güvenlik İlkesi yazarak Yerel Güvenlik İlkesi penceresini açın (04).



04

Hesap İlkeleri'ne , ardından da Hesap Kilitleme İlkesi'ne tıklayın. Hesap Kilitleme Süresi'ne çift tıklayın ve açılan pencerede (05) bir süre, örneğin 1 saat, seçin ve ardından Tamam'a tıklayın. Ardından Hesap Kilitleme Eşiği'ne çift tıklayın, 3 veya 5'i seçin. Bu, şifrenizin 3 veya 5 kez ard arda yanlış girilmesi durumunda bilgisayarınızın 1 saat kilitleneceği anlamına gelmektedir.



05

Not: Bir sonraki adıma geçmeden önce, Win10 için kullanıcı adınızı ve Win10 hesabınızla bağlantılı e-posta adresinizi bildiğinizden emin olun, gerekiyorsa bir kenara yazın. Bu değişiklikleri gerçekleştirdikten sonra hesabınıza girmek için bu bilgilere ihtiyacınız olacak.

Yerel İlkeler > Güvenlik Seçenekleri' ne gidin. Etkileşimli oturum açma: En son kullanıcı ismini görüntüleme'ye çift tıklayın ve Etkin'i seçin. Etkileşimli oturum açma: Oturum kilitletiğinde kullanıcı bilgisini görüntüleme'ye çift tıklayın ve Kullanıcı ismini görüntüleme'yi seçin (06).



06

Bu, bilgisayarınız başlatıldığında kullanıcı isminizin görüntülenmeyeceği ve Windows'u açmak için hem kullanıcı isminizi hem de şifrenizi birden girmeniz gerekeceği anlamına gelmektedir. Bunu güvenliğinizi arttırmak için kullanabilirsiniz.

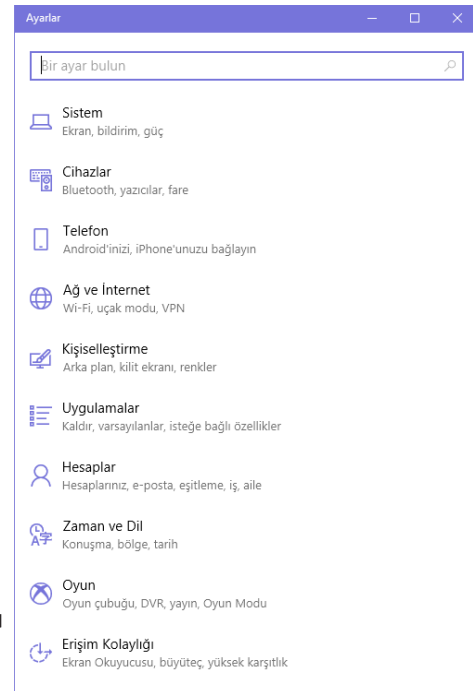
Son olarak, yukarıdaki aynı Yerel Güvenlik İlkeleri (Yerel ilkeler > Güvenlik Seçenekleri) penceresindeki Kapatma: Sanal bellek sayfadosyasını temizle seçeneğini bulun, Etkin'i seçin ve Tamam'a tıklayın. Bunun nedeni Bölüm 7: Bilgiyi silme kısmında görülebilir.

AYARLAR (SETTINGS)

Bu temel ayarlar (07) uygulamaların ve programların konum hizmetlerini kullanmalarına veya webcam ve mikrofonun çalışmasına izin vermayla alakalıdır. Ayrıca bu ayarlar güvenliğinizi arttırmak için çeşitli değişiklikleri yapmanızı da mümkün kılar.

Güncellemeler (Windows Update settings). Gelişmiş Seçenekler'e tıklayın; Otomatik güncellemeleri, ve ardından da "Windows'u güncellediğimde başka Microsoft ürünleri için bana güncellemeler ver"i seçin.

Windows Defender (Windows Defender). Gerçek Zamanlı koruma'yı ve Bulut Bazlı koruma'yı açın. Eğer bir başka Anti-Virüs programı kullanıyorsanız Windows Defender otomatik olarak kapanacaktır, bu nedenle bu adımı atlayabilirsiniz.



07

Yedekleme (Backup Settings). Yedekleme Dosya Geçmişini kullanıyor seçeneğinin işaretli olmadığından emin olun.

Konum (Location privacy settings). Konum'un devre dışı bırakıldığından emin olun. Buradayken Bu cihazdaki geçmiş temizle seçeneğine tıklayın. Akıllı telefonunuzun aksine, bilgisayarınızda konum özelliğinin açık olmasına neredeyse hiçbir zaman gerek olmayacaktır.

Webcam (Webcam privacy settings). Webcam'inizi nadiren kullanıyorsanız (08) bu hizmeti kapatın. Eğer sık kullanıyorsanız açık bırakın, fakat aşağıya inerek tüm programların üzerinden geçin ve kullandığınız program haricindeki (örneğin Skype) tüm programların webcam erişimini devre dışı bırakın.

Aşağıda görüldüğü üzere, Webcam ayarlarındaki gibi bir hizmeti tamamen kapatmak yerine bazı programlar için erişilebilir kılmayı Mikrofon, Kişiler vb. kalemler için de kullanabilirsiniz.

Mikrofon (Microphone privacy settings). Mikrofonunuzu nadiren kullanıyorsanız bu hizmeti kapatın. Eğer sık kullanıyorsanız açık bırakın, fakat aşağıya inerek tüm programların üzerinden geçin ve kullandığınız program haricindeki (örneğin Skype) tüm programların webcam erişimini devre dışı bırakın.

Cortana (Cortana & Search settings). Tüm seçenekleri kapatın. Bu Win10'nun bir arama fonksiyonudur ve yaptıklarınıza dair fazlasıyla bilgi toplayan bir hizmettir. Bu nedenle bu fonksiyonu kapalı tutmak en iyisidir.

Oturum (Account info privacy settings). Oturum Bilgisi'ni kapatın.

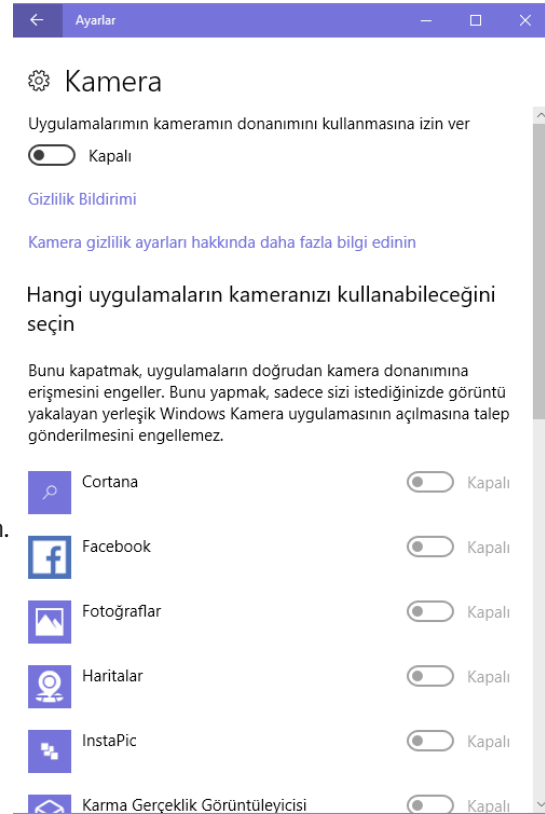
Kişiler (Contacts privacy settings). Kişiler'e erişimi olan tüm programları gözden geçirin ve gerekmeyen veya kullanılmayan her şeyi devre dışı bırakın.

Aynı bölümde (Privacy settings), Genel, Takvim, Arama Geçmiş, E-posta, Mesajlaşma, Radyolar ve Diğer Cihazlar seçeneklerini bulun. Bunlar arasından kullandığınıza yüzde yüz emin olmadığınız her şeyi kapatın.

Geri Bildirim & Tanılama (feedback settings) seçeneği altında, Windows geri bildirimim için bana danışsın'ı Asla'ya ve Microsoft'a cihaz verilerinizi gönderin'i Temel'e ayarlayın.

Giriş yapma seçeneklerinizi (sign-in options) gözden geçirin ve bilgisayarınızı uykudan uyandırmak için şifre gerektiğine emin olun.

Başlatma ayarlarınızı (start settings) kontrol edin ve Başlat'taki veya göre çubuğundaki En çok kullanılan uygulamaları göster, yakın zamanda eklenen uygulamaları göster ve yakın zamanda açılan kalemleri göster seçeneklerini devre dışı bırakın.



08

Bluetooth (Bluetooth settings) açın ve Bluetooth'u kullanmadığınız takdirde kapatın. Bluetooth'u kullanmaya karar verdiğinizde, Daha fazla Bluetooth seçeneği bağlantısına. Açılan yeni pencerede Bu PC'yi bulmak için başka Bluetooth cihazlarına erişim verin seçeneğini devre dışı bırakın. Ardından Yeni bir Bluetooth cihazının bağlanma isteğinde beni uyarın seçeneğini seçin.

Bilgisayarınıza uzaktan erişime izin verin' i arayın ve erişim izni olmadığından emin olun (Remote Assistance and Remote Desktop).

Son olarak Arkaplan uygulamaları sekmesinin en altında, hangi uygulamaların arka planda çalışma iznine sahip olduğunu gözden geçirin ve kullanmadıklarınızı veya kullanılmasını istemediklerinizi kaldırın. Sohbet programlarını bilgisayarınızda kullandığınız takdirde, bu uygulamaların arkaplanda çalışması gerekmektedir (fakat sohbet programlarını bilgisayarınızda kullanmaktan mümkün mertebe kaçınmalısınız).

Tebrikler! Kılavuzun en sıkıcı kısmını tamamladınız. Şimdi daha ilginç bölümlere geçebiliriz.

BÖLÜM 2

BİLGİSAYAR GÜVENLİĞİ

ALT BÖLÜM 3 TEMEL KURALLAR



Dijital güvenliğin büyük bir kısmı düşündüğünüz kadar teknik değil. Daha çok teknolojiyi günlük işlerimizde nasıl kullandığımızla ve güvenlik çerçevesinde nasıl davrandığımızla alakalı. Bu bölümde güvenli davranışlara dair birkaç temel kural anlatıldı. Bahsi geçen davranışları bir anda hayatınıza uygulayabileceğinizden emin değilseniz, endişelenmeyin. Bu meseleleri ilerleyen bölümlerde daha detaylı şekilde tartışmaya açacağız. Fakat bu kurallar uzun bir yol gerektirebilir, bu kısa bölümü okurken ekstra olun. Böylelikle kılavuzun devamında burada anlatılanları aklınızda tutabilir, bunları uygulamada birer kriter olarak kullanabilirsiniz.

Temel kuralları okurken teker teker durup kendinize, bu kuralların kendi davranışlarınıza veya rutininize nasıl uygulanabileceğini sorun. Fazla karmaşık değil; fakat her temel kural hakkında detaylıca düşünmeye zaman ayırmanız, bu kuralların birbirleri ve rutininizle nasıl ilişkilendiklerini anlamanızı sağlayacak. Hali hazırda hem online, hem de offline olarak bu talimatları uyguluyor musunuz? Yanıt hayırsa, bu kuralları uygulamak için ne gibi değişiklikler yapmanız gerektiğini düşünün. Sorularınız veya şüpheleriniz varsa bunları not edin. Kılavuzun ilerleyen bölümlerinde bu soruları cevaplandırabilmeyi umuyoruz. Cevaplandırılmayan sorular için sizden gelen geri bildirimler ışığında kılavuza eklemeler yapacağız.

TANIYIN

Mevcut tehditlerin tamamından kendinizi korumanız pek mümkün değil. Denediyseniz bile bu mesele dönüşebilir; buna rağmen yüzde 100 korunmanız mümkün değil. Bunun yerine anahtar tehditlere odaklanın. Gerçekçi olun. İnsan hakları savunucuları, gazeteciler, hukukçular, STK çalışanları için bazı temel tehditler mevcut ve bunları burada sıralamaya çalıştık. Fakat teknolojinin farklı şekilde kullanılabileceğini iyice anlamak uzun bir yolculuk. Bu nedenle her şeyden önce ilk bölümü iyi okuyup anlamanız esas. Kendi durumunuzu oturup analiz etmeniz, nelere odaklanmanız gerektiğini kavramanız için önemli. Karşı karşıya olduğunuz tehditlerin sebeplerinin ve sonuçlarının neler olduğunu, nereden kaynaklandıklarını ve bunları ortadan kaldırmak –hiç olmazsa hafifletmek için neler yapmanız gerektiğini anlamaya çalışın. Kılavuzun sonuna doğru karşılaşılabileceğiniz tehditleri ve bunlara karşı kendi kabiliyetleriniz çerçevesinde neler yapabileceğinizi taslak haline getirebilmiş olmalısınız.

SADELEŞME, SADELEŞME, SADELEŞME

Bir uzman da olsanız, çok sayıda programı güvenle kullanabilmek, aksini yapmaktan daha zor. Her program yeni bir güvenlik riski demek. Telefonunuzdaki ve bilgisayarınızdaki tüm programlara bakın. Hepsini kullanıyor musunuz? Kullanmıyorsanız ya da gerçekten ihtiyacınız yoksa silin gitsin. Bir telefonda birçok anlık mesajlaşma programı gerçekten ihtiyacınız var mı? Muhtemelen yok. Bunu yapmanız cihazınızda yer de açacak.

UYGULAMALAR VE PROGRAMLARDAN KAÇININ

Çok güvenli açık-koddan yana birkaç grup hariç, kuvvetli şifrelemelere sahip firmalar, hizmetler ve programlar standart olmayabilirler. Programların standart halinde bulunduğu bir dili tercih etmeniz (özellikle İngilizce) sizin açınızdan daha korunaklı olabilir. Uygulamaların ve programların yerleştirilmesi eğer yazılımı üreten firma/grup tarafından yapılmamışsa, dil ve erişebilirlikten feragat ederek programı anadilinde (veya standardize olduğu bir dilde) kullanmanız sizin için daha yararlı olacaktır.

BOŞ GELEN KUTUSU

Açık konuşmak gerekirse e-postalarınıza dair bekleyen büyük risk e-postalarınıza olacak. Şifrenizi vermek zorunda kalabilirsiniz veya yazıştığınız bir başka kişi bunu çoktan yapmış olabilir, erişilebilir. İşte Boş Gelen Kutusu Politikası burada fazlasıyla işlevsel ve güvenliğiniz için en önemli araçlardan biri.

E-postanıza erişileceğini varsayın. Boş Gelen Kutusu Politikası okunacak hiçbir şey olmayacağını garantiler. Kısaca gelen kutunuzu olabildiğince boş bırakın. Çoğu zaman bu işlem hiçbir problem arz etmeyecek, zira büyük ihtimalle çoğu yazışmanızı saklamaya ihtiyaç duymuyorsunuz. Bunun önemini ne kadar anlatsak az. Bu politikayı iş arkadaşlarınız veya dostlarınızın da uyguladığından emin olun. Bu konu Bilgi Paylaşımı bölümünde daha detaylı tartışılacak.

Size tıpkı Telegram ve Signal gibi güvenli, yüksek şifreleme seviyesine ve otomatik silme fonksiyonuna sahip bir e-posta hizmetini de tanıtacağız.

CEVAPLAMAMA ANLAŞMASI

Cevaplamama Anlaşması, Boş Gelen Kutusu Politikası'nın daha geniş hali. Eğer e-postalarınıza erişildiyse, üçüncü kişiler sadece bekleyerek haberleşme ağınıza dair fazlasıyla bilgi alabilir. Çünkü bu durum e-postaları nasıl kullandığımızla alakalı. Çoğunlukla yazışırken yeni bir e-posta yazmaktansa var olan bir e-postayı 'cevaplarız'. Bu sayede aynı e-postada geçmişteki yazışmalar da görünür. Bu yazışmalar çok uzun bir zamana yayılır ve bu nedenle ufacak bir yeni cevap, uzun bir geçmişi barındırıyor olabilir.

Cevapla fonksiyonundan olabildiğince uzak durun. Kullandığınız takdirde, orijinal metni silin. Bu alıkondüğunuz süre içinde olabildiğince az bilgiye erişilebilmesi demek. Bu sayede Boş Gelen Kutusu Politikanıza karşı bir hamle de yapılamaz. Bilgi Paylaşımı bölümünde buna dair daha

detaylı bilgi bulabilirsiniz. İletişimde olduğunuz insanlarla konuşun ve cevapla fonksiyonundan uzak durmaya çalışın.

DURUM PLANLARI

Elektronik cihazlarına bir kez el konduğunda , artık geç kalmışsınız demektir. Hatta bu andan sonra alacağınız önlemler, aleyhinize kullanılabilir. Önceden hazırlıklı olmalı, öncesi, sırası ve sonrasında neler yapacağınızı bilmelisiniz. İş arkadaşlarınızın ve dostlarınızın ne yapacağını da. BİR PLANA İHTİYACİNİZ VAR. Bu da bunu önceden konuşup planlamaktan geçiyor. Ortak bir mutabakatınız olmalı. Hepiniz fabrika ayarlarına geri mi döneceksiniz? Şifrelerinizi mi değiştireceksiniz? Bilgisayarınıza format mı atacaksınız? Önemli olan herkesin aynı şeyi yapıyor olduğundan emin olmak.

Bu bir 'güvenlik protokolüne' sahip olmak uygulamak demek. Çabalarınız kişisel kalıyorsa, girişimleriniz anlamsızlaşabilir, sizi ya da başkalarını riske atabilir. Bu konuyu konuşun. Unutmayın, eğer aığınız birden fazla kişi ve çalışma grubunu içeriyorsa, hele de bu kişiler ya da gruplar birbirlerini tanımıyorlarsa, hatta kimileri daha savunmasızsa, farklı gruplar için farklı acil durum planları oluşturun. Bunun paranoyaklık olduğunu düşünmeyin. Bu konuyu Bölüm 12: Engelleyici Güvenlik bölümünde daha geniş inceleyeceğiz.

Devam etmeden önce Bölüm 2: Bilgisayarınızı Hazırlama bölümündeki talimatları uyguladığınızdan emin olun. İlerleyen bölümlerdeki daha teknik ve davranışsal güvenlik adımlarını düzgünce atabilmek için temel meseleleri güvenli hale getirmek önemli bir gereklilik.

BÖLÜM SONU SORULARI

- Boş gelen kutusu politikası ne ve neden önemli?
- Cevaplamama anlaşmasını korumak neden önemli?
- Güvenlik yazılımlarını güncellememek neden riskli?
- Acil durum planı ne?
- Bir acil durum planı tasarlamak için hangi adımları atmak gerek?
- Kullandığınız programları neden azaltmalısınız?

PRATİK DİJİTAL GÜVENLİK

ALT BÖLÜM 4 BİLGİYİ EDİNME



Bu bölüm size güvenli şekilde bilgiye nasıl erişebileceğinizi öğretecektir. Nasıl bilgi aramanız, tarayıcınızı ve tarayıcınızla birlikte kullandığınız internet bağlantısını tartışacaktır. Güvenliğiniz için hem tarayıcınızı hem de tarayıcınızın internette çevrim içi olması için kullandığı bağlantıyı bir arada düşünmelisiniz. Bağlantınızı güvenli hale nasıl getireceğinizi bilmek aynı zamanda sansür sınırlarını da aşmanızı mümkün kılacaktır.

Mobil cihazlar üzerine yazılmış III uygulamalara ve mobil cihazlara daha çok odaklanmaktadır. Bu kısım daha çok dizüstü bilgisayarlar içindir.

Tarayıcı nedir? Tarayıcılar web’de dolanmak için kullandığımız uygulamalardır. Yaygın tarayıcılara Safari, Firefox, Chrome, Opera ve İnternet Explorer örnek olarak verilebilir fakat seçebileceğiniz daha bir çok tarayıcı da bulunmaktadır. Bazıları güvenlik açısından diğerlerinden daha üstündür.

Çevrimiçiyken, ziyaret ettiğiniz web sayfaları hakkınızda bilgi toplar. Aynı zamanda bilgisayarınız da tarayıcınızda yaptığınız işler hakkında bilgi toplar. Bunu “çerezlerinizi”, “Yerel Paylaşımlı Nesneleri (LSOs)”, girdiğiniz şifreleri, tarayıcı geçmişinizi kullanarak yapar. Bu durum sizin için farklı yollarla zayıf noktalar oluşturabilir. Hepsinden öte, çoğu web sitesi komut dosyaları (scripts) kullanır (Javascript programlama) ve bu yolla tarayıcınız ve web bug’lara (tarayıcınız yoluyla bilgisayarınıza bulaşan virüsler) maruz kalabilir. Bu iki meseleyi de çözmek gerekmektedir.

TARAYICI

İdeal olarak bir tarayıcınızı, kapandığı her sefer yaptığınız her şeyi otomatik olarak silecek şekilde ayarlamanız gerekmektedir. Bu güvenliğinizi artırır. Fakat, kişisel amaçlarla ne kadar çok kullandığımızı düşününce, her hizmet için tekrar tekrar oturum açmamızın (örneğin eğlence veya online alışveriş hizmetleri için) gerekmesi çok verimsiz olacaktır. Burada çift tarayıcı stratejisi önerilmektedir. Bir tarayıcınızı kişisel internet kullanımında, bir başkasını da işlerinizi gerçekleştirmede kullanın. İş için Firefox kullanmanızı öneririz. En hızlı tarayıcı olmayabilir fakat çok önemli kişiselleştirme ayarlarına sahiptir ve bunların bir kısmı önemli güvenli uzantıları ve add-on’larıdır. Bunlar ileride daha detaylı biçimde anlatılacaktır.

Kişisel kullanım için Chrome veya Opera tercih edebilirsiniz. Çift tarayıcı kullanımı kişisel kullanımınızın uzantılar veya add-on’larla yavaşlamayacağı, beri yandan işinizle ilgili internet kullanımınızın da güvenli olacağı anlamına gelmektedir.

Karar, bu karara sadık kalın. Sadece işle ilgili kullanın; araştırma, e-posta vb. işlerinizi burada gerçekleştirin. Diğer tarayıcınızı ise sörf amaçlı kullanın. İki'den fazla tarayıcı yüklemeyin. İki tarayıcı seçin ve bunlara sadık kalın. Aşağıdaki kısımlar size Firefox'u daha güvenli nasıl kullanacağınıza dair daha nitelikli bilgiler verecektir.

DOSYALARI DOĞRU YERDE KAYDETMEK

İlerideki Firefox üzerine olan kısım bunu nasıl yapacağınızı size gösterecektir. Öncelikle indirme konumunu manuel olarak seçmenin neden önemli olduğunuzu anlamanız gerekiyor. Tarayıcınızın varsayılan indirme/kaydetme klasörü, çok az insanın dikkate aldığı büyük bir güvenlik riskidir. Fakat bunu düzeltmek kolaydır.

Hiçbir değişiklik yapmadığınız takdirde, indirdiğiniz herhangi bir ek veya belge İşletim Sisteminizin (OS) sabit diskinde depolanacaktır. Peki bu neden bir problem? Bölüm 5: Bilgiyi Depolama ve Bölüm 7: Bilgiyi Silme bölümlerinin de göstereceği üzere, aslında bilgiyi tam anlamıyla silmek çok güçtür. Bu konuda ayrıntılara ileride değineceğiz. Şimdilik sadece tarayıcınızın indirdiğiniz dosya ve eklentileri nereye kaydedeceğini belirleyeceksiniz.

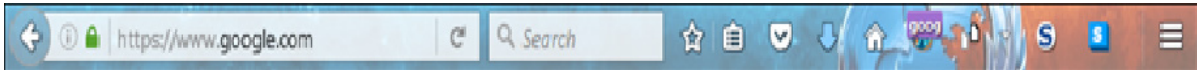
Öncelikle Dosyaların nereye kaydedileceğini her zaman bana sor'u seçmelisiniz. Böylelikle herhangi bir dosya indirdiğinizde, dosyanın nereye kaydedileceğini tarayıcınız size soracaktır. Ardından şifreli bir disk ayarladığınızda (Bölüm 5: Bilgiyi Depolama bölümünde anlatılacaktır), hassas veya işle ilgili indirmelerinizi doğrudan bu şifreli diske kaydetmelisiniz.

Belirli kişilerce erişilmesini istemediğiniz her türlü belgeyi otomatikman masaüstünüze kaydetme alışkanlığından kaçınmalısınız. Şifreli disklere kaydedildikleri durumda bu belgeleri güvence bilgisayarınızdan kaldırmak çok daha kolaydır, çünkü basitçe belgeleri silmek çoğunlukla yeterli olmamaktadır. (Daha fazla bilgi için bkz. Bölüm 7: Bilgiyi Silmek)

İNTERNET BAĞLANTISI

HTTP'YE KARŞI HTTPS

Günümüzde Facebook, Gmail, online bankacılık vb. oturum açmayı gerektiren çoğu hizmet, verdikleri hizmetle sizin aranızda şifrelendirilmiş bir bağlantı kullanmaktadır. Bağlandığınız bir siteyle aranızda şifreli bağlantı olduğunu anlamanın çok kolay bir yolu vardır. Tek yapmanız gereken tarayıcınızın adres çubuğuna bakmaktır (09)



09

Şifrelendirilmemiş bağlantılar HTTP ile başlamaktadır (http://www...). Şifreli bağlantılarsa HTTPS ile (https://www...) Firefox'un Heryerde HTTPS eklentisini kullanarak, mümkün olan her yerde tarayıcınızın https kullanmasını otomatikman sağlayabilirsiniz.

NASIL ÇALIŞIR?

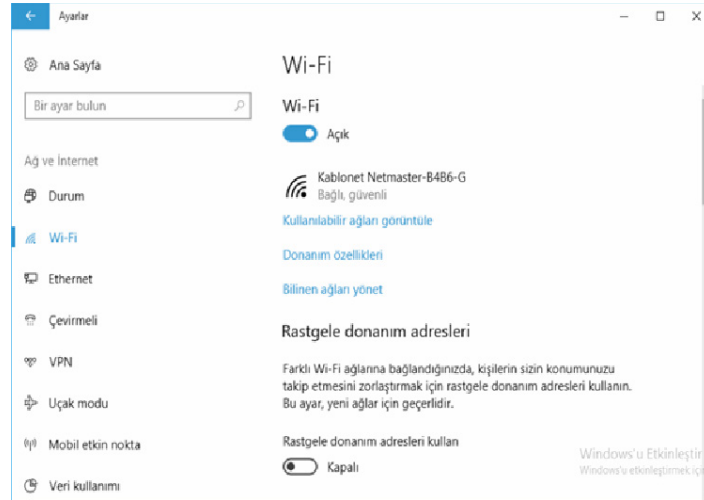
İnternete bağlandığınızda, router'ınız (evinizdeki veya ofisinizdeki internet trafiğini yöneten kutu) İnternet Hizmet Sağlayıcı'nızla (ISP) iletişime geçer ve bunu kullanarak size internete bağlar. Çeşitli sitelere erişimin engellenmesi İnternet Hizmet Sağlayıcı'nız aracılığıyla gerçekleştirilir.

İnternetinizin başkalarının izlenmesi (İster İnternet Hizmet Sağlayıcı'nız, ister ziyaret ettiğiniz siteleri, ister bilgisayarınızın/telefonunuzun bağlantı için kullandığı hizmetler tarafından olsun), IP adresiniz ve MAC adresiniz aracılığıyla gerçekleştirilir.

IP adresiniz, internet bağlantınızın adresidir ve kolaylıkla teşhis edilerek size karşı kullanılabilir. Kablosuz bağlantıları kullandığınızda IP'niz değişecektir (dinamik) fakat İnternet Servis Sağlayıcı'nız kimin nerede ne zaman hangi IP adresini kullandığını her zaman bilecektir. Burada VPN çok kullanışlıdır: VPN aracılığıyla etkin bir biçimde IP adresinizi değiştirebilir veya maskeleyebilirsiniz. Bu size ek bir anonimlik ve güvenlik katmanı kazandırırken, diğer yandan da İnternet Hizmet Sağlayıcı'nız tarafından internetin engellenmiş kısımlarına erişmenizi sağlar.

Cihazınızın veya bilgisayarınızın ayrıca bir MAC adresi vardır. Bağlantıya sahip her cihazın bir MAC adresi vardır ve bu eşsiz MAC adresi, donanımın kendisi için ayarlanmıştır. MAC adresi donanım üretildiğinde belirlenir ve kabaca şöyle görünür: 00:0a:95:9d:68:16. Fakat internete bağlandığınızda MAC adresiniz paylaşılmaz, bu nedenle bu konuda çok kafa yormanıza gerek yoktur. Öte yandan IP adresiniz sizin için sorunlara neden olabilir.

Win 10'da, Rastgele donanım adresleri (MAC) başlığında bir ayar vardır; buna sahipseniz etkinleştirin (10). Etkinleştirmenin ardından bağlantınızda sıkıntılar yaşıyorsanız, bilgisayarınızı yeniden başlatın. Sorun devam ediyorsa, tekrar devre dışı bırakın.



10

Neyse ki İnternet Hizmet Sağlayıcı'nızın hareketlerinizi izlemesinin veya sitelerinin gerçek IP adresinizi tespit etmesinin önüne geçmenin daha kolay yolları bulunmaktadır. Bu çözümler VPN ve TOR'dur; bu iki kaleme dair daha fazla bilgi aşağıda verilmiştir. Kısaca bir VPN veya TOR İnternet Hizmet Sağlayıcı'sını baypas ederek size doğrudan Türkiye'nin dışındaki sunuculara bağlar ve ayrıca çoğu zaman trafiğinizi şifreler; böylelikle İnternet Hizmet Sağlayıcı'nız İnternet kullanımınızı takip edemez. Türkiye'de birçok insan erişime kapalı sitelere girmek için bir çeşit VPN kullanıyor olsa da, VPN'nin aynı zamanda güvenlik ve gizlilik için de önem teşkil ettiğini unutmamak gerekir.

İNTERNET: ROUTER'İNİZ

İster evimizde, ister ofisimizde, istersek de bir kafede neredeyse her zaman internete kablosuz olarak bağlandığımızı söylemek mümkün. Bu nedenle kablosuz modemlerin ve router'ların nasıl çalıştığına dair temel bir kaç bilgi edinmemiz gerek.

Router'a erişmek için bir kullanıcı adı ve şifreye ihtiyacınız vardır. Bunlar çoğunlukla modeminizin (router'ınızın) arkasına yazılmıştır. Neredeyse her modem için bunlar "admin" ve "şifre" formundadır. Farklı bir formda yazılmış olsa da, aynı markaya ait veya aynı modeldeki her modem aynı kullanıcı ismine ve şifreye sahiptir, bu nedenle bunları tespit etmek çok kolaydır. Bu bilgiye dayanarak üçüncü kişiler modeminize bağlanabilir. Bu üçüncü kişiler, internetinizi kontrol eden modeminize bağlandıkları takdirde kolaylıkla yaptığınız her şeyi kaydedebilen bir programı sisteminize yükleyebilir, hatta internetinizi engelleyebilirler. Çoğu kullanıcı modeminde girerek kullanıcı adını ve şifresini değiştirmeye uğraşmaz. Modeminize erişim çoğunlukla tarayıcınızı açıp, adres çubuğuna IP adresinizi yazarak gerçekleşebilir (Bu IP adresi çoğu zaman 192.168.0.1'dir). Bu yolu kullanarak modeminize girebilir, kullanıcı adınızı ve şifrenizi değiştirebilirsiniz.

Dikkat edilmesi gereken bir başka anahtar mesele de kablosuz internet kullanırken, kablosuz sinyallerin şifrelenmesi gerektiğidir. Aksi takdirde buy olla iletilen her şey yakındaki herhangi biri tarafından görüntülenebilir. Şifrelendirilmediği takdirde kablosuz ağınıza herkes bağlanabilir, bu ağı kullanabilir, hatta bu bağlantıda yapılan tüm işleri kaydedebilir. Kablosuz ağınızın bir ismi vardır ve buna SSID denir. Kablosuz bir bağlantıya bağlanmak bir şifre istiyorsa, bu bağlantı şifrelendirilmiştir (encryption). Şifre yoksa, şifrelendirme de yoktur.

Modeminize girdiğinizde, ağınızın adını değiştirebilirsiniz (SSID) ve hatta sinyallerinizi şifrelendirebilirsiniz. Wi-Fi modemlerde günümüzde kullanılan standart şifrelendirmeye WPA2 adı verilir. Daha eskileriyse WEP olarak bilinmektedir. Bunları kullanmayın. Şifrelendirme için bir şifreye karar vermelisiniz.

Bu yüzden modeminize girmek için bir kullanıcı adı ve şifre bulunmaktadır. Ardından, kullandığınız asıl kablosuz sinyaller için bir isim ve şifre vardır. Bu ikisi aynı şeyler değildir. Modeminizde bu değişiklikleri yapabilmeyi anlamak için biraz yardıma ihtiyacınız olacaktır; basitçe modeminizin adını ve model numarasını google'layın. İnanın fazlasıyla yardıma erişeceksiniz. Modeminizin arayüzü karmaşık gözükse de sadece bir kaç ufak şeyi değiştirmeniz yeterlidir ve inanın bu işlem görüldüğünden çok daha kolaydır.

VPN'LER VE TOR

VPN (Virtual Private Network) kullanmak sadece internet trafiğinizi/bağlantınızı şifrelediği için bilgilerinizi İnternet Hizmet Sağlayıcı'nız tarafından erişimi engellemekle, aynı zamanda İnternet Hizmet Sağlayıcı'nızın aşmanızı sağlar. Ayrıca ziyaret ettiğiniz sitelerinin gerçek IP adresini kaydetmelerini de güçleştirir. Hassas olduğunu düşündüğünüz meseleler üzerinde çalışırken mutlaka VPN'niniz açık şekilde çalışmalıdır. Fakat böyle bir alanda değilseniz, VPN'ninizi kapatmanızı öneriyoruz zira bazı insanlar sürekli ve gereksizce VPN kullandıkları için fazladan ilgi çektiklerini belirtmektedirler. Bu önemli bir dengedir ve bu dengeye en sağlıklı olarak ancak kendiniz karar verebilirsiniz.

Bazı VPN'lerin acil anahtar (kill switch) denilen ve VPN'ninizin çalışmaması durumunda otomatik olarak internet bağlantınızı kesen araçları vardır (böylelikle VPN bağlantınız düştüğünde kullandığınız sitelerinin veya hizmetlerin gerçek IP'nizi görmesi engellenir). Bunu kullanmanız önerilmektedir. Günümüzde bir çok VPN gayet kuvvetlidir ve hız olarak çok büyük farklar görmeyeceksinizdir. İyi bir VPN edinmek bir miktar paraya mal olabilir fakat bu parayı yapabileceğiniz en önemli yatırımlardan biri olarak görebilirsiniz.

VPN bilgisayarınızı/sunucunuzu doğrudan Türkiye'nin dışında (burada bağlanmak istediğiniz noktayı seçebilirsiniz; ister Avrupa, ister Amerika, veya dünyanın herhangi başka bir yeri...) bir sunucuya, bir 'tünel' yaratarak İnternet Hizmet Sağlayıcı'nızı baypas etmek yoluyla bağlar. Ziyaret ettiğiniz web siteleri, VPN yoluyla bağlandığınız sunucunun IP adresini görecektir, size ait asıl IP adresini değil. Böylelikle İnternet Hizmet Sağlayıcı'nız internet trafiğinizi kontrol etmekten mahrum kalır, daha da ötesi yaptıklarınızı kayıt altına alamaz veya erişmek istediğiniz siteleri engelleyemez. VPN kısaca İnternet Hizmet Sağlayıcı'nızı pas geçer. Bu, fiziksel olarak Türkiye'de olmanıza rağmen, bilgisayarınızın Amerika'da, Avusturalya'da veya Almanya'da olması anlamına gelir.

Astrill güçlü bir VPN sağlayıcısıdır; ekstra güvenlik hizmetlerine ve dünya çapında sunuculara sahiptir. VyprVPN ve ExpressVPN de diğer popüler seçenekler arasındadır. İnternette buna dair araştırmalar yapmak da VPN servisleri arasında karşılaştırmalar yapmanızı sağlar. Güncel, iyi çalışan VPN'lerin listesi için Google'ı kullanın. Bol bol bilgiye ve karşılaştırma yorumlarına buradan ulaşabilirsiniz. Türkiye'de çoğu insan ücretsiz VPN'ler kullanıyor olsa da, bu sistemler çoğunlukla ücretli VPN'ler kadar fazla fonksiyona ve seçeneğe sahip değildirler. Ayrıca dönem dönem başkalarınca kapatılma veya saldırıya uğrama tehlikesiyle karşı karşıyadırlar. Eğer ciddi anlamda çevrimiçi anonimliğiniz, güvenliğiniz ve erişim özgürlüğünüz kaygıya düşüyorsanız, bir VPN'i satın almayı gözden geçirin.

VPN kullanmak IP adresinizi korumak için iyi bir araçtır, fakat tamamen güvenli değildir. Bir miktar kaynak harcayarak başkaları size bululabilir. İnterneti gerçekten hassas işler için kullandığınızda, TOR'u kullanmalısınız.

TOR'un açılımı The Onion Router'dır. Tıpkı VPN gibi TOR (bu hizmet ücretsizdir), kullandığınızda nihai adresinize ulaşmadan önce sizi dünya çapında bir çok sunucudan geçirerek aradığınız websitesine götürür. Mevcut en güvenli iletişim yoludur. Çok güvenilirdir fakat çok da yavaştır. TOR'da video izlemeyi unutun. Eğer size veya çevrenizdekilere karşı gerçekten kullanılabilir hassaslıkta herhangi bir şey yapacak olursanız, TOR kullanmanız en iyi seçenek olabilir. Hem bilgisayarınıza hem de telefonunuza yüklemek çok kolaydır (eğer cihazınız güncellenmiş durumdaysa).

Onion router (Soğan modem) adıyla anılmasının nedeni, bir çok farklı sunucudan sunucuya (20 sunucuya kadar) atlayarak sizi ziyaret ettiğiniz adrese götürmesindedir; tıpkı bir soğanı katman katman soyarak gibi. Bir çok sunucuyu kullanmasından ötürü, internet kullanımınızı takip ederek IP adresinize ulaşmak neredeyse imkansız hale gelir.

DUCKGOGO.COM VE SÖRF

DuckGoGo bir arama motorudur, tıpkı Google gibi. Diğerlerinden farklı olarak DuckGoGo arama sonuçlarınızı konumuza, geçmiş aramalarınıza dayandırmaz ve kullanıcılarına dair hiçbir veriyi elinde tutmaz. Daha güvenli bir sörf yöntemidir zira zaman içerisinde size dair veri toplamaz. Bu reklamlardan kurtulmanızı, daha da önemlisi geçmiş aramalarınıza, konumuza ve daha bir çok parametreye dayanarak size özel verilen reklamları atlamanızı sağlar. DuckGoGo sadece İngilizce'dir fakat çok basit bir arayüze sahiptir; bu nedenle kısıtlı bir İngilizce'ye sahip olmanız ciddi bir problem teşkil etmeyecektir.

TOR / TOR browser ile DuckGoGo'yu birlikte kullanıyorsanız, gezintilerinizden geriye neredeyse hiçbir şey kalmayacaktır; ne İnternet Hizmet Sağlayıcı'nızda ne de ziyaret ettiğiniz sitelerinde. Eğer size problem yaratabileceğini düşündüğünüz herhangi bir bilgiyi araştırıcaksanız, DuckGoGo'yu TOR tarayıcı'da

(browser) kullanın. Maksimum güvenlik için TOR tarayıcı'yı bir USB stick'ten kullanın; bu bilgisayarınızda depolanan izleri de sınırlayacaktır.

İnternet gezintileriniz mevzu bahis olduğunda güvenlik seviyeleri şu şekilde özetlenebilir:

TOR en iyi güvenliği sunar. Bu seviye VPN kullanmaktan daha yüksektir fakat VPN'de olmak 'normal' bağlantıya nazaran çok daha güvenlidir. Tarayıcı seçmek konusunda USB'de bulunan bir TOR tarayıcı kullanmanız en güvenli yöntemdir. Düzgünce ayarlanmış bir Firefox kullanmak, 'normale' ayarlı bir tarayıcı kullanmaktan daha güvenli ve iyidir.

TEKNİK ÇÖZÜM: FIREFOX VE UZANTILAR


Eğer Firefox'a sahip değilseniz, Firefox.com'dan indirip hemen yükleyin. Yükleme işlemi ister sabit diskinize isterseniz de bir USB'ye gerçekleştirilebilir. Yüklemenin ardından yapacağınız ilk iş bir kaç eklenti ve uzantıyı Firefox'a yüklemek olacaktır.

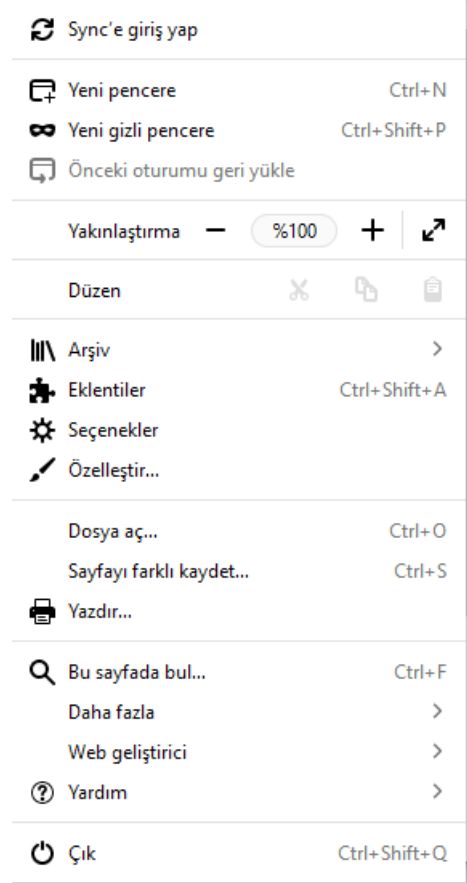
UZANTILAR

Eklentiler kısmına Firefox'taki Ayarlar'a (Settings) tıklayıp Eklentiler (Add-ons) butonunu seçerek ulaşabilirsiniz (11). Buradan yüklemek istediğini eklentileri aratabilir ve hali hazırda yüklü bütün eklentileri sıralayan bir sekme ulaşabilirsiniz (Bu sekme Uzantılar (Extensions) denmektedir). Burada ayrıca her eklenti için ayrı ayrı Seçenekler (Options) de bulabilirsiniz.


Aşağıdaki eklentileri bulup yükleyin;


- RefControl,
- NoScript,
- BetterPrivacy,
- HTTPS Everywhere, ve
- KeyScrambler.

 Refcontrol. Bir websitesini ziyaret ettiğinizde, websitesi nereden geldiğinizi görebilir. Örneğin Google'dayken Facebook'a geçerseniz Facebook, sayfalarına Google üzerinden ulaştığınıza dair bir bilgi alacaktır. Buna 'başvuran' (referrer) denir ve bunlar insanların sitelerine nasıl ulaştığını analiz etmede kullanılır. RefControl'u yükleyerek bir kaç basit tıklamanın ardından bu durumun önüne geçebilirsiniz. Yükleme işleminden sonra Seçenekler'e (Options) tıklayın ve pencerenin en altında Default for sites not listed diyen kısımda Forge veya Block'u seçin.



11

 NoScript. Bu program otomatik olarak tarayıcınızda Javascript'in çalışmasını engeller. Bu çok önemlidir çünkü bir çok virüs farkedilmeden script'ler yoluyla cihazlarınıza bulaşır. Bu eklenti hareket ettirebilen grafikleri, otomatik video tekrar oynamayı ve daha nicelerini devre dışı bırakır. Bunun yerine tarayıcınıza bir simge bırakır. Eğer bulunduğunuz siteye güveniyorsanız ve script'leri çalıştırmasını istiyorsanız, bu simgeye tıklayıp allow (izin ver) seçeneğine tıklamanız yeterli olacaktır. Eğer bulunduğunuz websitesi düzgün yüklenmiyor veya çalışmıyorsa, bunun nedeni muhtemelen bazı script'leri engellemiş olmanızdır. Bu noktada yine allow seçeneğini seçmelisiniz. NoScript için başka değişikliklere ihtiyaç yoktur.

 BetterPrivacy. Bu eklenti yükleyerek, tarayıcınızı kapattığınızda otomatik olarak silinecek veriler hakkında daha fazla seçeneğe sahip olabilirsiniz. Sadece bu eklenti yükleyerek, silinmesi güç olan bir çerez tipi olan LSO'lardan (Local Shared Objects – Yerel Paylaşımlı Nesnelere) kurtulabilirsiniz. Yüklemenin ardından Options (Seçenekler) tuşuna tıklayın ve ardından Options & Help (Seçenekler ve Yardım) sekmesini seçin. Delete Flash cookies on Firefox exit tuşuna tıklayın. Ayrıca Also delete Flashplayer default cookie ve On cookie deletion also delete empty cookie folders seçeneklerine de tıklayın.

S HTTPS Everywhere. Bazı siteleri bilgisayarınız ile websitesi arasındaki iletişimde şifreleme kullanır: Örneğin bankalar, e-posta sağlayıcıları, bazı sosyal medya siteleri vb. Bu ilave bir güvenlik katmanıdır. Günümüzde daha fazla websitesi HTTPS sağlıyor olsa da bu durum evrensel değildir ve bu hizmeti sağlayan bazı siteler de otomatik olarak sağlamamaktadır. Bu eklenti, HTTPS şifreleme sunan sitelerinde bu hizmetin otomatik olarak başlamasını sağlar. İndirdiğiniz zaman, Firefox araç çubuğunda bir simge göreceksiniz. Buna tıklayıp Enable HTTPS Everywhere seçtiğinizde otomatik olarak çalışmaya başlayacaktır.

Yukarıdaki eklentilerin haricinde, aşağıdaki eklenti 'eklentiler bölümü' aracılığıyla yüklenemez. Bunun yerine download.com'a gidin ve KeyScrambler'ı arayın. İndirmek için bunu seçin ve normal bir program gibi yükleyin. Programın çalışması için bilgisayarınızı yeniden başlatmanız gerekecektir.

K KeyScrambler. Tarayıcınıza kullanıcı isimleri veya şifreleri girdiğinizde bastığınız tuşları şifreleyen küçük bir programdır. Gelişmiş hack yöntemleri bilgisayarınıza bir keylogger programı yerleştirebilir. Bu keylogger'lar bilgisayarınızda bastığınız tüm tuşları sırasıyla kaydeder ve bilgisayarınıza bu programı sokan kişi yazdığınız her şeyi sırasıyla görebilir; kullanıcı isimleriniz ve şifreleriniz dahil. Oturum açma ve şifre girme sırasında bastığınız tuşları şifreleyerek bu program otomatik olarak bu konuda sizi korumaya alacaktır.

Bunları yükledikten sonra (S-W/O2), lütfen Firefox'un uzantılar/eklentiler dükkanında biraz daha zaman geçirin ve varolan programları incelemeye koyulun. Burada kendi güvenliğinize, verimliliğinize ve üretkenliğinize uygun başka yararlı eklentiler bulabilirsiniz. Ayrıca Google'da Firefox için En Güvenli Eklentiler (Best Security Add-ons for Firefox) veya benzeri bir cümle aratarak, size uygun olabilecek yeni eklentiler de bulabilirsiniz.

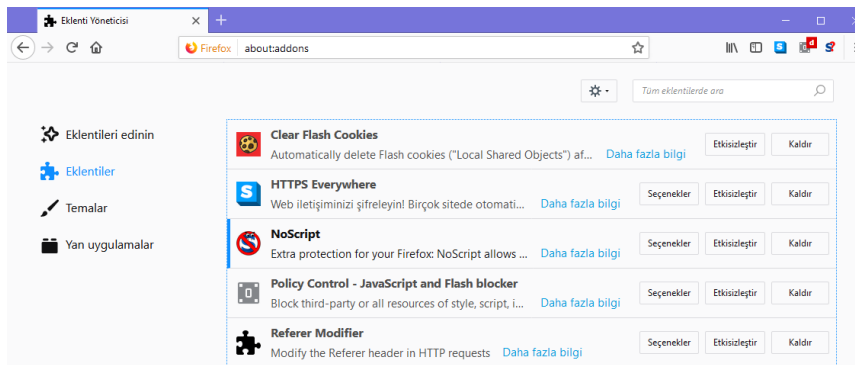
Tarayıcınızı güvenli kılmada yolu yarlıdınız. Şimdi ayarlarda bir kaç ufak değişiklik yapmalıyız.

AYARLAR VE SEÇENEKLER

Firefox'u ve eklentilerini yükledikten sonra sıra tarayıcınızın ayarlarına bir göz atmakta ve her şeyin güvenli bir seviyeye ayarlandığını kontrol etmekte. Ayarlar (Settings) tuşuna tıklayın ve ardından Seçenekler'ı (Options) seçin. Seçenekler bölümünde bir kaç sekme bulunmaktadır. Burada adı geçen her sekme için bazı değişiklikler gerçekleştirilmelidir.

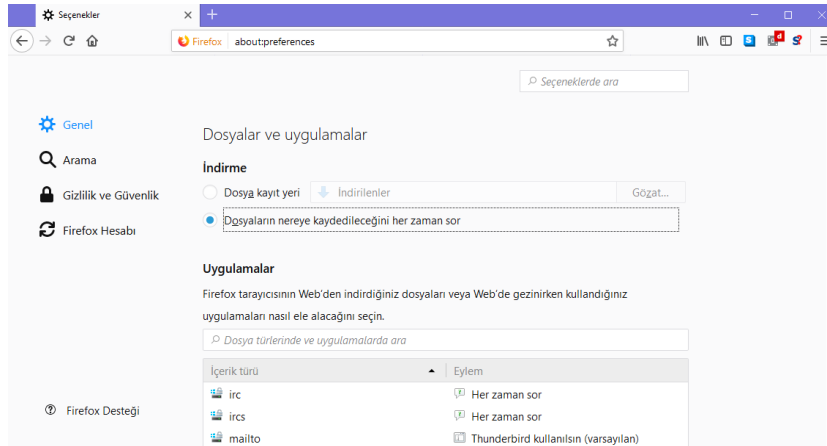
UZANTILAR (EXTENSIONS)

Yüklediğiniz farklı uzantılar için seçeneklere göz atarak işe başlayın. Bunların çoğu baştan ayarlı gelmektedir ve değişime ihtiyaç duymazlar fakat varolan seçenekler konusunda fikir edinmeniz için buraya göz atmanız her zaman önemlidir (12).



GENEL (GENERAL)

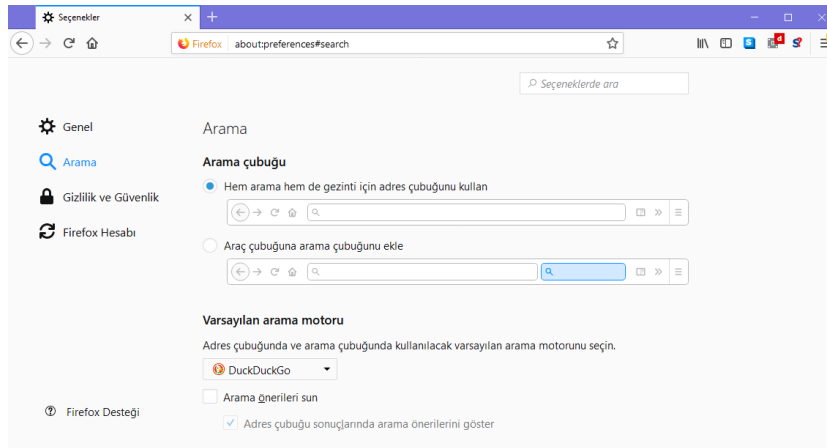
Dosyaların nereye kaydedileceğini her zaman sor'u (Always ask me where to save files) seçin. (13).



13

ARAMA (SEARCH)

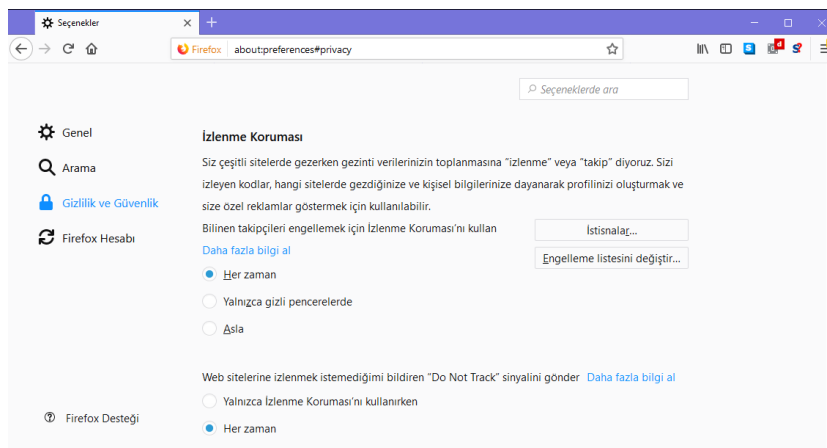
Arama önerileri sağla'nın (Provide search suggestions) seçili olmadığından emin olun (14).



14

GİZLİLİK (PRIVACY)

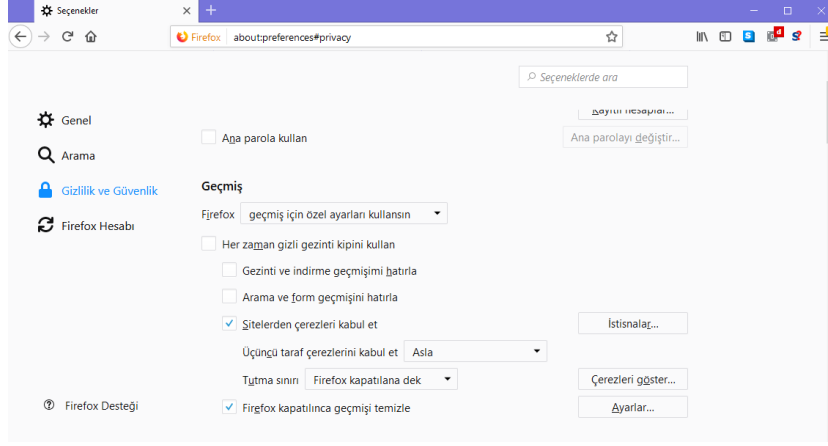
Özel Pencerede İzlenme Koruması Kullan (Use Trackin Protection in Private Window) seçeneğini etkinleştirin. Geçmiş'in altında Geçmiş Asla Hatırlama'yı (Never Remember History) seçin. Konum Çubuğu (Location Bar) altında hiçbir şeyin seçili olmadığından emin olun. (15)



15

GÜVENLİK (SECURITY)

Güvenlik (Security) sekmesi altında (16), Genel (General) kısmında görünen üç kutuyu seçin ve Oturum Açma (Logins) kısmını altındaki iki kutucuğun işaretinin kaldırıldığından emin olun (Siteler için oturumları hatırla ve Master şifre kullan). Buradayken 'Kayıtlı Oturumlar'a (Saved Logins) tıklayın ve herhangi bir şeyin kayıtlı olup olmadığına bakın. Eğer kayıtlıysa, silin.



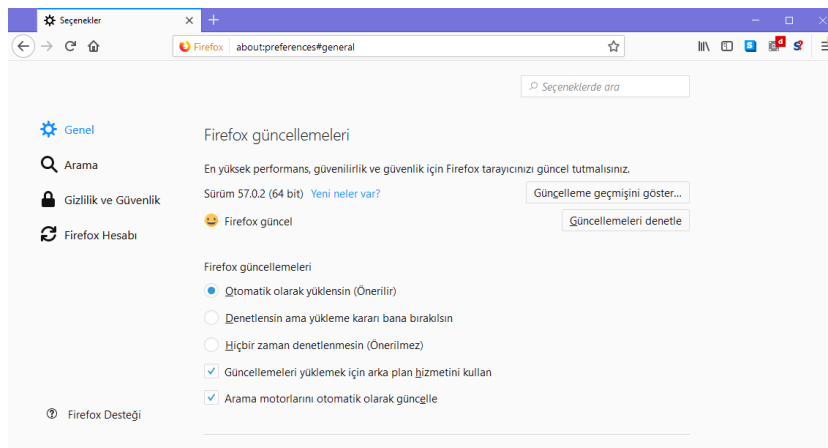
16

SENKRONİZASYON (SYNC)

Senkronizasyonu kullanmayın ve Firefox'u herhangi bir e-posta hesabı veya benzeriyle bağlamayın. Firefox'a e-posta hesabınızla kayıt olmayın!

GELİŞMİŞ (ADVANCED)

Veri seçenekleri (Data choices) altındaki üç kutunun da işaretinin kaldırıldığından emin olun. Ağ (Network) altında Otomatik önbellek yönetimini geçersiz kıl'ı (Override automatic cache management) seçin ve buraya 50 yazın. Son olarak Güncelleme (Update) sekmesi altında Otomatik olarak güncellemeleri yükleyin (Automatically install updates) seçin. Ayrıca Arama Motorları'nın da (Search Engines) otomatik güncelleme yaptığından emin olun. (17)



17

TEKNİK ÇÖZÜM: TOR

Unutmayın; TOR internette sadece basit işleri yaparken güçlü bir güvenlik sunar. Çünkü TOR bağlantınızı bir şey izlemek, yayınlamak veya büyük dosyaları indirmekten aciz kılacak kadar yavaşlatır.

TOR Tarayıcı'yu (bir program/uygulama) ister bilgisayarınıza, ister doğrudan bir USB'ye yükleyebilirsiniz. Basittir ve başlattığınızda otomatik olarak çalışmaya başlar. Bundan kastımız sadece spesifik bir tarayıcının TOR kullanıyor olmasıdır; bilgisayarınızın geri kalanı değil. Eğer tüm bilgisayarınızın TOR kullanmasını istiyorsanız programı indirip yüklemeniz gerekmektedir. Bunu yaparsanız tüm bağlantılarınız TOR tarafından sağlanacaktır: örneğin diğer tarayıcılarınız, arkaplan bağlantı verileri, Skype, vb.

TOR tarayıcı için <https://www.torproject.org/projects/torbrowser.html.en> adresine gidin ve işletim sisteminize ve dile bağlı olarak kullanacağınız tarayıcıyı seçin. TOR ayrıca mobil uygulamalar da üretmektedir.

Dosyayı yüklemek istediğiniz konuma indirin; bu konum ister bir USB, ister gizli şifrelenmiş bir sabit disk olabilir. Eğer gizli şifreli bir sabit diskiniz veya belleğiniz henüz yoksa, Bölüm 5: Bilgiyi Depolama'da anlatıldığı üzere gizli şifreli bir bellek kurun ve bu bölüme sonrasında geri dönün.

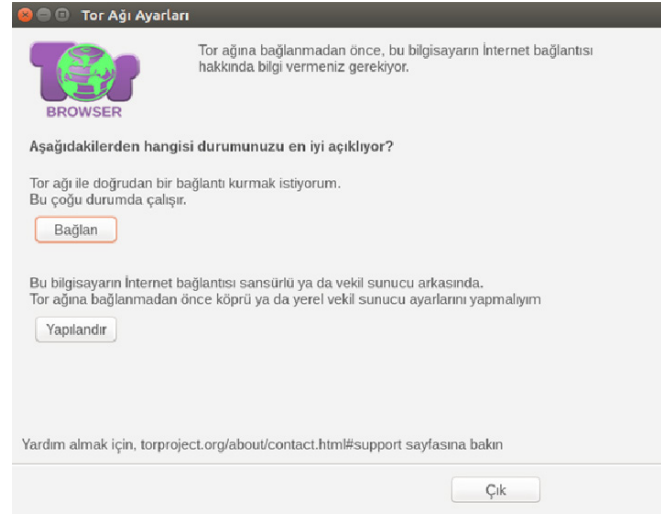
Tor Browser Downloads

To start using Tor Browser, download the file for your preferred language. This file can be saved wherever is convenient, e.g. the Desktop or a USB flash drive.

Stable Tor Browser			
Language	Microsoft Windows (6.0.5)	Mac OS X (6.0.5)	Linux (6.0.5)
English (en-US)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
العربية (ar)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Deutsch (de)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Español (es-ES)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
فارسی (fa)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Français (fr)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Italiano (it)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
日本語 (ja)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Korean (ko)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Nederlands (nl)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Polish (pl)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Português (pt-PT)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Русский (ru)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Türkçe (tr)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Vietnamese (vi)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
简体字 (zh-CN)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)

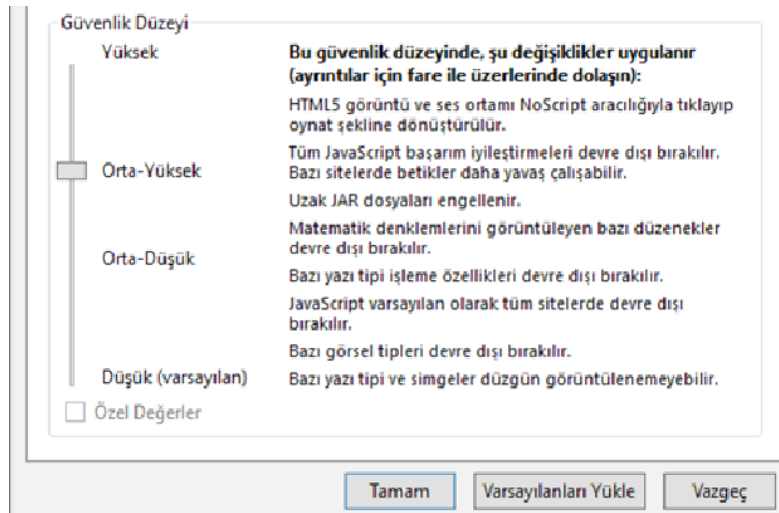
Normal sabit diskiniz haricinde ister bir USB'te (aşağıya bakınız) ister şifreli bir sabit diske programı yükleyebilirsiniz. Yüklemenin ardından hali hazırda çalışan herhangi bir VPN'niniz varsa kapatın ve TOR'un çalışıp çalışmadığını test etmek için engelli bir websitesine girin.

Bir programı başlattığınızda, bağlanmak için iki seçeneğiniz bulunmaktadır. İsterseniz ilkin Doğrudan Bağlantı (Direct Connection) kullanmayı deneyin; en kolayı bu seçenektir (18). Bu seçimi TOR'u ilk kez başlattığınızda yapacaksınız; bundan sonraki kullanımlarda TOR seçiminizi ve ayarlarınızı hatırlayacak, normal bir tarayıcı gibi çalışacaktır. TOR tarayıcı Firefox tabanlıdır ve Seçenekleri Firefox'a çok benzerdir. TOR tarayıcıyı ilk kez çalıştırdığınızda, Seçenekler bölümüne gidin, ve aşağıdaki Firefox ve Uzantıları ekinde gösterildiği üzere Firefox için verilmiş talimatlarla aynı seçimleri yapın.



18

TOR'la bir başka ayar bölümüne daha sahipsiniz. Adres çubuğundan önce Yeşil bir Soğan Simgesi göreceksiniz. Buna tıklayın ve Gizlilik ve Güvenlik Ayarları'nı (Privacy and Security Settings) seçin (19).



19

Tüm kutuları işaretleyin. Ayrıca güvenlik seviyesinizi ayarlayabildiğiniz Güvenlik Seviyesi (Security Level) kaydırma çubuğuna da dikkat edin. Başlangıç için bunu Yüksek seviyeye ayarlamayı öneriyoruz.

Eğer çeşitli websiteleri düzgün çalışmıyorsa bu seviyeyi, sitelerin çalışabildiği bir güvenlik seviyesine düşürebilirsiniz.

Öneminden ötürü tekrar hatırlatmakta fayda görüyoruz: Eğer TOR Tarayıcı kullanıyorsanız, sadece bu tarayıcının trafiği TOR'dan geçmektedir. Bilgisayarınızdaki başka veri iletimleri TOR'dan geçmez!

USB'DE TOR

TOR ayrıca bir USB'ye yüklenebilir. Bu yolla USB'yi sadece USB'yi bilgisayarınıza bağlayıp, TOR üzerinden çevrimiçi olan özel tarayıcıyı başlatabilirsiniz. USB kullandığı için, kullandığınız bilgisayarda internetinizden geri küçük izler bırakır. Küçük bir USB alıp TOR'u buraya yüklemeyi gözden geçirin. Bu USB'yi dosya saklamak gibi başka bir eylem için asla kullanmadığınızdan emin olun. Yükleme süreci yukarıda anlatılanla aynıdır: Tek yapmanız gereken indirilen dosyayı USB'nize kaydetmek ve programı USB üzerinde yüklemektir. USB'ye yüklense dahi tarayıcı aynıdır ve yukarıda bahsedilen değişiklikleri yine yapmanız gerekmektedir. Tarayıcıyı kullanmadan önce mutlaka Ayarlar bölümüne bir göz atın ve yukarıda bahsedilen değişiklikleri yapmayı ihmal etmeyin.

PRATİK DİJİTAL GÜVENLİK

ALT BÖLÜM 5 BİLGİYİ DEPOLAMA



Bu bölüme iki farklı tip şifrelemeyi göstermektedir. İlki, Temel Şifreleme, bilgisayarınızda veya herhangi bir USB'de yerleşik olan otomatik şifrelemedir. Bu şifreleme günümüzde akıllı telefonların kullandığı şifrelemeye benzer yapıdadır. İkincisi ve daha önemli olan şifreleme biçimi ise, sabit diskinizin veya bir USB'nin bir alanında gizli, fazlasıyla şifrelenmiş (Gelişmiş Şifreleme) yaratmaktır. Bu alanda işinizle ilgili hassas dosyaları tutacağınız varsayılmaktadır.

Şifreleme günümüzde sıkça kullanılan bir kelimedir ve e-postadan chat programlarına, internete erişimden bilgilerinizi depolamaya kadar uzanır. Şifreleme, verinin başkaları tarafından okunamayacak şekilde korunması anlamına gelir. Bu veriyi sadece şifrelemede kullanılan anahtara sahip kişiler okuyabilir (bu işleme şifre çözme denir). Bu bölüm sabit diskler, USB'ler gibi depolama amaçlarınız için veri şifrelemeye spesifik olarak odaklanmaktadır. E-posta, internet bağlantısı vb. başlıkların şifrelenmesini içermez.

AŞIRI KURTULMA

Daha farklı sabit disklerde ve cihazlarda daha fazla veri depolamanız, verilerinizin korunmasını güçleştirir. İlk adımınız, işinizle ilgili verileri nerede depolayacağınıza karar vermek ve bu karara sadık kalmak olmalıdır. İkinci adımsa artık ihtiyaç duymadığınız her şeyden kurtulmak olmalıdır. Eğer gerçekten bir veriye ihtiyacınız yoksa, kurtulun gitsin. Korumanız gereken veri ne kadar az olursa işiniz o kadar kolaylaşacaktır.

Karşılaşacağınız riskleri nasıl sınırlandıracağınızı sürekli olarak analiz etmeniz gerekecektir. Ayrıca güvenliğinizin herhangi bir katmanı kırıldığında bu risklerden kendinizin, çalışma arkadaşlarınızın veya sizin korumanız altında çalışan insanların nasıl etkileneceğini de analiz etmeniz gerekmektedir. Unutmayın; bu meseleyi aynı zamanda iş arkadaşlarınızla veya dayanışma ağınızla da tartışmanız gerekmektedir. Ancak bu yolla onların güvenliği aşıldığında nasıl risklerle karşı karşıya kalacağınızı anlayabilirsiniz. Örneğin şifrelenerek depolanmış iş dosyalarınızın gizliliği ifşa edildiğinde, bu ihlali gerçekleştiren tarafın hangi bilgiye erişimi olacaktır; isimler, kaynaklar, hassas konumdaki bireylerin adresleri, siz ve ortaklarınız arasındaki ayrıcalıklı iletişim?

Daha az bilgiyi tutmanız, size zarar vermek isteyenler tarafından edinildiği durumda daha az bilgiye dair endişe duymanız anlamına gelir. Bu da sadece gerçekten ihtiyacınız olan bilgiyi tutmaya özen göstermeniz demektir. Kürt'lere yönelik dair uzun bir rapor yazdığınızda, ciddi miktarda araştırma, not ve röportaj üretilecektir. Suriyeli sığınmacı gazetecilerin eğitimine dair bir plan/önerge ürettiğinizde, bir çok isme ve yere dair bilgiye ihtiyaç duyacaksınız. Seks işçileri için ruh sağlığı desteği sağlamaya yönelik bir proje geliştirdiğinizde, kimliklerinin başkalarının eline geçmesini istemediğiniz birçok katılımcı veya destekçinin bir listesi elinizde olacaktır. Çoğunlukla iş sürecimiz boyunca, son ürünü ortaya çıkarana kadar bir çok belge yaratırız; tablolar, çizimler, word belgeleri, kontak listeleri vb. Nihai belgeyi tamamladığınızda, diğer tüm dökümanları elinizde tutmaya gerçekten ihtiyacınız var mıdır? Bu durum risk analizinizde nerede durmaktadır? En muhtemel sonuçta olacağı gibi bunlardan kurtulun ve sadece son dökümanı kaydedin ve depolayın. Bölüm 7: Bilgiyi Silmek kısmı, güvenlice bilginin nasıl silineceğine dair detayları ortaya koymaktadır.

DEPOLAMA NE KULLANMALI

HDD, SSD, SD, USB. Bu terimler ortalıkta dolaşanlardan sadece bazılarıdır. Bu kavramlar farklı depolama biçimlerini temsil etmektedir. Kullandığını depolama tipi, artık ihtiyacınız olmayan bilgiyi silmeniz gerektiğinde bunu ne kolaylıkta ve ne düzgünlükte yapacağınızı doğrudan etkiler. Bu noktada çalışma belgelerinizi depolamak için ne tip depolamayı kullanacağınıza karar vermeden önce, Bölüm 7: Bilgiyi Silme kısmının HDD'ye karşı SDD kısmını okumak iyi bir fikir olabilir. Bu Gelişmiş Şifreleme kurduğunuz zaman önem kazanacaktır. Fakat öncelikle aşağıdaki Temel Şifreleme bölümünü okuyup üzerinden geçebilirsiniz.

TEMEL

Eğer bir iPhone veya bir Android telefon kullanıyorsanız, bu telefonların hali hazırda etkinleştirilmiş şifrelemelerle satıldıklarını fark edeceksinizdir. Olmadığı takdirde dahi bu telefonları şifrelemeniz mümkündür ve tek yapmanız gereken bir PİN kodu veya şifre seçmenizdir (ve bu süreçte varolan hiçbir bilgi silinmeyecektir).

Günümüzde Win10 ve OSX'te de aynı fonksiyonu bulabilirsiniz. Bu sistemler kolaylıkla bilgisayarınızın bir sabit diskini (disklerini) şifrelemenizi bir PİN kodu veya şifre seçmek yoluyla mümkün kılar. Telefonların aksine bunlar, bilgisayarınızı almanızla birlikte gelmez, bu nedenle bunları kendiniz yapmalısınız. Bu şifrelemeyi etkinleştirmek hard diskinizi formatlamaz/silmez veya bilgisayarınızda her hangi bir şeyi ortadan kaldırmaz. Şifrelemeyi etkinleştirdiğiniz andan önce bilgisayarınızda ne bulunuyorsa yerli yerinde kalacaktır ve hiçbir değişiklik görmeyeceksinizdir.

Temel Şifreleme herkes tarafından kullanılmalıdır çünkü verilerinizi çok kolay bir yolla korur. Kullanıcı olarak sizin için fark çok küçüktür. Şifreleme etkinleştirilirse, bilgisayarınızı veya telefonunuzu başlattığınızda PİN kodunuzu veya şifrenizi girmeniz gerekecektir. Bunu yapmazsanız cihazınız başlatılmaz çünkü sabit diskinize erişimi engellenir ve dolayısıyla İşletim Sisteminizi (OS) başlatamaz. Bu tip şifrelemeyi harici diskler, USB'ler vb. için de gerçekleştirebilirsiniz (bu durumda cihazları bilgisayarınıza bağladığınızda size bir şifre veya PİN kodu sorulacaktır.)

Çoğu telefonun ve bilgisayarın açılmak için bir şifreye veya PİN koduna ihtiyaç duyduğunu göz önüne alınırsa, burada farkın ne olduğunu merak edebilirsiniz. Burada fark alıştığınız eski tip şifre veya PİN kodu girme işlemi, bilgisayarınızın veya telefonunuzun arayüzünün açmaya (kilit ekranından İşletim Sistemi'nin

arayüze geçme) yarayan tiptedir. Bu şifreler sadece İşletim Sisteminiz'in yüklenmesinden ve çalışmasından sonra sizden istenir ve eğer başka biri bilgilerinize erişmek istiyorsa basitçe sabit diskinizi veya kullandığınız başka bir depolama cihazını alıp, başka bir bilgisayara bağlayarak içerisindeki her şeyi okuyabilir. Cihazı veya sabit diski şifrelemek bunu engeller

Kilit ekranından arayüze geçişte şifre kullanmanız, evinizdeki kapılar gibidir. Şifrelemeyse bu kapıların kilitlerine benzer. Kilidi olmayan bir kapı, içeriye biri girmek istediğinde pek de güvenli sayılmaz.

EK: Temel Şifreleme, bunu bilgisayarınızda nasıl etkinleştireceğinizi gösterir. Bu özelliğe BitLocker denir. Fakat bunu sadece Win10 PROFESSIONAL sunmakta, HOME sürümüyse bu özelliğe sahip değildir. HOME sürümüne sahipseniz bunu kullanamazsınız, dolayısıyla EK: Gelişmiş Şifreleme bölümüne atlayabilirsiniz.

Eğer OSX'iniz eskiyse –tıpkı Win10 HOME kullanıcıları gibi, bu özelliği kullanamazsınız. Budurumda EK: Gelişmiş Şifreleme bölümüne atlayınız.

VE ÇALIŞMA DOSYALARINIZIN DEPOLANMA

Temel Şifreleme bilgisayarınızda temel bir güvenlik sağlar. Kullanıldığı halde, gelecekte bilgisayarınızı başlatırken bir şifre veya PİN kodu kullanmanız gerekecektir, hepsi bu. Bundan sonra daha sofistike adımları konuşacağız; burada çalışma dosyalarınızı depolayacağınızı ve tutacağınızı varsayıyoruz. Temel Şifreleme kullanmasanız dahi bu gizli şifreleme, çalışma dosyalarınızı güvenli ve gizli tutacaktır. Kullanacağımız program Veracrypt veya Truecrypt olacaktır. Win10 ve OSX'te bu iki program da aynı şekilde çalışmaktadır.

Çalışma dosyalarınızı için güvenli, gizli bir şifreleme alanı yaratacağız. Sıfır Gelen Kutusu Politikası'nda önceden gösterildiği üzere, anahtar tehdit başkalarının çok gelişkin hack yöntemleri kullanarak şifrelemelerinizi kıracağı değil, üçüncü tarafların sizden şifrenizi zorla aldığı durumda ne olacağıdır. İnternette gezintideki ve kullandığınız e-postadaki gibi önemli güvenlik meselesi, bu bilgiye sahip olduğunuzu bilmemeleridir; çünkü başkası sizden var olduğunu bilmediği bir bilgiyi isteyemeyecektir.

Bu sorunu aşmanız için çok kolay ve akıllıca bir yöntem vardır: gizli şifreleme. Burada amaç bilginin varlığından kimsenin haberdar olmayacağı, dolayısıyla kimsenin sizden zorla şifrelerinizi alamayacağıdır. Sıfır Gelen Kutusu Politikası ve Bölüm 7: Bilgiyi Silme kısmıyla birlikte bu bölüm, kılavuzun en önemli bölümüdür. Bunların kombinasyonu sizi asıl koruyacak olan husustur. Ve en baştan belirtelim: Kullanımı ne karmaşık, ne de güç. Belki kurmak için bir miktar zaman harcamanız gerekecektir fakat kurulduktan sonra tek yapmanız gereken bir tuşa basmak olacaktır.

Açıklanacağı üzere, sadece dosya şifreleme uygulamasının bilgisayarınızda bulunuyor olması bile şüphe çekeceği için bir stratejiye ihtiyacınız olacak. Sıkça kullanılan bir strateji bazı materyallerin, örneğin yasaklı bir kitap veya filmin, hatta pornografinin, dış katmanda şifrelenmiş bir sürücüde tutulmasıdır. Bu sayede saklamanız gereken ufak tefek şeylerin olduğu ilizyonunu yaratabilir, sizi veya başkalarını ciddi risklerle karşı karşıya getirecek daha hassas belgeleri bir başka yerde saklamaya devam edebilirsiniz. Bahsettiğimiz dış katmanı bir yem gibi düşünebilirsiniz; fakat bu yemin inanılabilir olması gerekmektedir. Ayrıca burada kendinizi veya başkalarını çok daha büyük risklere atmaktansa, daha risksiz bir durumu göze aldığınızı farkında olmanız gerekmektedir.

BU NE YARATIR?

Bir sabit disk veya bunun bir kısmı veya bir USB vb. şifrelendiğinde, bilgisayar bu kısmı okuyamaz. Okuyabilmek için öncelikle onun şifresini çözmeniz gerekmektedir (bir şifre girerek). Teknik analiz yaparak kötü niyetli taraflar şifreleme kullandığınız kanaatine varabilir (veya sabit diskinizin zarar gördüğü kanaatine varabilirler). Bunu takiben sizden zorla şifrenizi edinmeye çalışabilirler. Bundan kaçınmanın bir yolu yoktur. Fiziksel tehditler çoğunlukla efektiftir.

Bu sorunu aşmanın bir yolu tek bir şifreleme değil, aynı alanda iki hatta daha fazla şifreleme yaratmaktadır. İlk şifreleme alanınıza burada Dış katman, ikinci veya üçüncü şifreleme alanlarınıza da İç katman diyoruz. Katman, şifrelenmiş alan için verilmiş bir başka isimdir. Bir şifre Dış katmanı açmaya yararırken, diğer (ve çok daha güvenli) bir şifre İç katmanı açmaya yarayacaktır. Şu anda gizli şifreleme kullanıyorsunuz.

İç katmanın bir Dış katmanın içinde olmasından ötürü, hiçbir teknik analiz yolu karşınızdakilere İç bir katmana sahip olduğunuzu gösteremez.

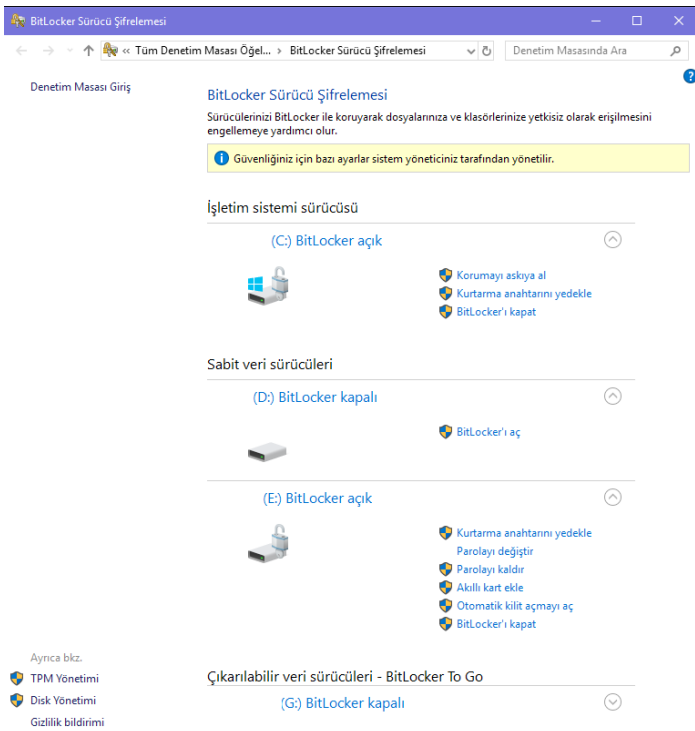
Pratik nedenlerden ötürü şifrelenmiş alanınızı yüklemeniz gerektiğinde, girdiğiniz ilk şifre Dış katmanı açacaktır. Dış katman bir yem gibi çalışacaktır: Burada amacınızın kötü niyetli tarafların sizi şifrenizi vermeye zorladığı, bu yolla şifrenizi edindiği ve şifrelenmiş katmanınıza eriştiği durumlarda, erişecekleri bilginin çok büyük hassaslıklar içermeyeceği, fakat bu kişileri de şifrelenmesi gerek bir bilgiye ulaştıkları yönünde tatmin edeceği nitelikte olmasıdır. Dış katmana bir takım belgeler yerleştirmelisiniz, böylelikle sizden bu katmanı açmanızı istediklerinde aradıkları şeyi bulduklarına inanacaklardır. Beri yandan asıl önemli bilgilerinizi daha gizli, iç katmanda tutmaya devam edebileceksiniz.

TEKNİK ÇÖZÜM: TEMEL ŞİFRELEME

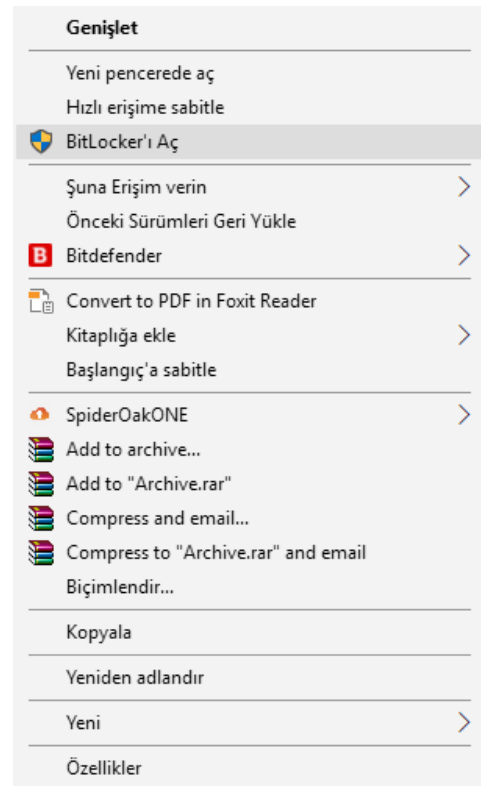
Win10'nun kendisinde bulunan ve şifreleme yapan programı BitLocker'dır. Bu programı arama çubuğunda aratarak başlatabilirsiniz. İşletim Sistemi'nizi, sabit diskinizi, harici disklerinizi ve USB'lerinizi bu programla şifreleyebilirsiniz.

Eğer görürseniz, TPM denilen bir şeyi açmanız gerekmektedir. Bu işlemi ekranlardaki adımları izleyerek yapabilirsiniz. İşlemin sonunda bilgisayarınızı yeniden başlatmanız gerekecektir. TPM açılmasına dair daha fazla bilgi edinmek için google'ı kullanın: İşinize yarayacak fazlasıyla bilgi burada mevcuttur.

BitLocker'ı başlattığınızda, ana menüden şifrelemek istediğiniz sabit diskleri veya çıkarılabilir aygıtları (USB'ler, SD kartlar vs.) seçebilir veya Explorer penceresinde diske sağ tıklayıp BitLocker'ı Aç (Turn On BitLocker) sekmesini seçebilirsiniz (20, 21). Başlamadan önce kısa süreliğine kullanmak üzere etrafınızda bir USB veya yazıcı olduğundan emin olun.



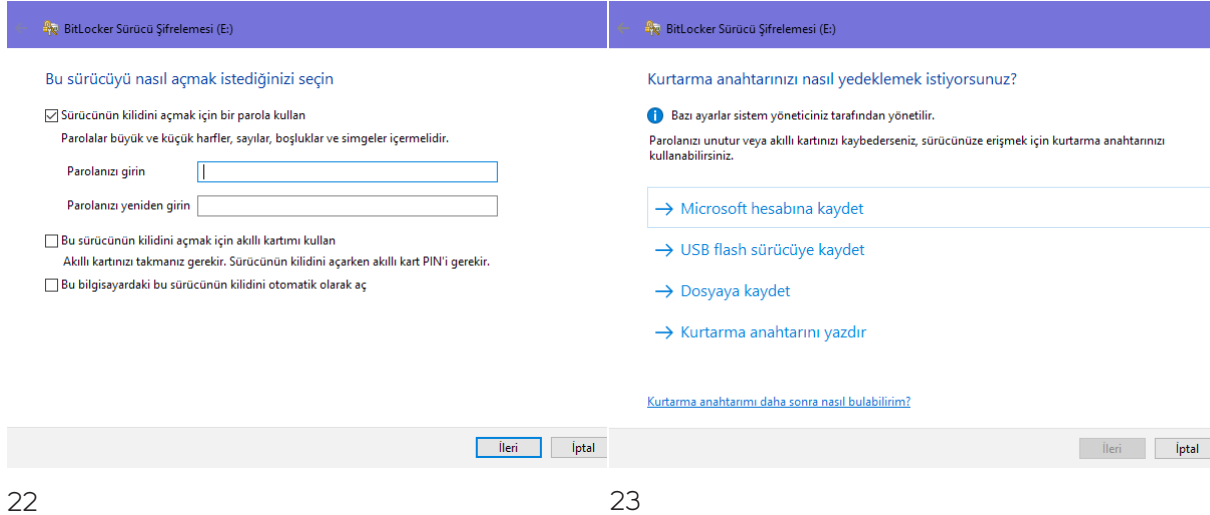
20



21

BitLocker'ı Aç'a tıklayarak herhangi bir sabit disk veya USB için süreci başlatın. İlk adımda şifrelenmiş diskinizi nasıl açacağınızı seçeceksiniz; burada Bir şifre kullan (Use a password) seçmelisiniz (22) ve devam tuşuna basmalısınız. Bu temel şifreleme olduğundan, bir PİN kodu veya kısa bir şifre kullanabilirsiniz.

Ardından Geri Alma anahtarınızın nerede saklanması istediğiniz sorusunu göreceksiniz. Karakterlerden oluşan bu anahtar, şifrenizi kaybettiğiniz veya unuttuğunuz durumlarda şifrelenmiş diskinizi açmak için kullanabilirsiniz. Bu çok büyük bir güvenlik tehditidir. Bunu önlemek için bir yazıcınız varsa Geri alma anahtarını yazdır'ı (Print the recovery key) seçin. Eğer yazıcınız yoksa, Bir dosyaya kaydet'i (Save to a file) seçerek şimdilik bir USB'ye kaydedin (23). Ayrıca bunun bir kopyasının da Windows oturumunuzda Microsoft tarafından depolanmasını da seçebilirsiniz fakat windows oturumunuza online olarak erişildiği durumda, bu erişimi sağlayan herhangi biri tarafından diskinizin şifrelenmiş hali şifre gereksinimi olmadan çözülebilir.



Dolayısıyla bu seçeneği sadece Windows oturumunuzu koruyabileceğinize kesin inanıyorsanız kullanın.

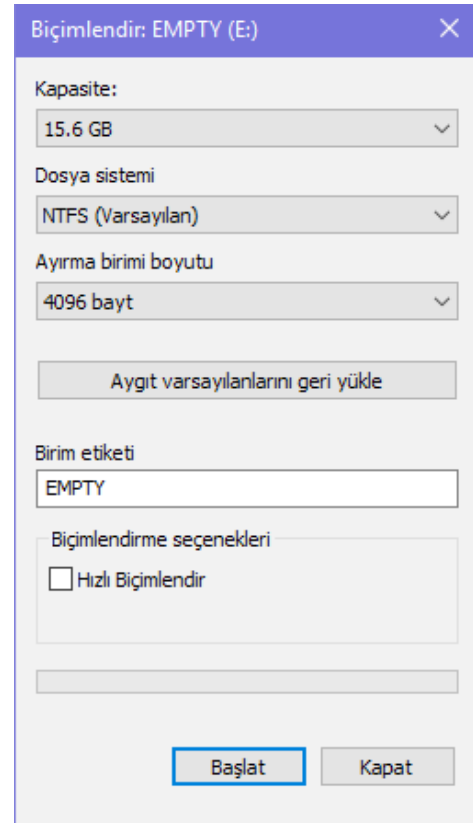
Geri Alma dosyasını kaydettikten ve İleri tuşuna tıkladıktan sonra, sabit diskinizin veya USB'nizin ne kadarının şifrenmesini istediğiniz sorulacaktır. Burada her zaman Tüm sürücüyü şifrele (Encrypt entire drive) seçeneğini işaretleyin. İlerleyen sayfada yeniden size en uygun şifrelemeyi seçmelisiniz; genellikle Yeni şifreleme modu (New encryption mode) en iyisidir fakat ikinci seçenek Uyumluluk modu (Compatible mode) da bu işlemi, Windows sisteminin en son sürümüne sahip olmayan başka bilgisayarlarda da kullanmak istediğiniz bir USB veya harici disk üzerinde gerçekleştirdiğiniz durumda seçilebilir.

Şimdi diskinizi şifrelemeye hazırsınız. Şifrelemeye başla (Start encrypting) tuşuna tıklayın ve işlemin arka planda gerçekleşmesine izin verin. Sabit disk ne kadar büyükse işlem o kadar uzun sürer. Bu bir arkaplan sürecidir; dolayısıyla bırakın arkaplanda işini yapsın.

Son olarak Geri Alma dosyasından kurtulmamız gerek. Eğer çıktısını aldıysanız, kağıdı yok edin. Böylece şifreniz okunamaz. Eğer bir USB'ye kaydettiyseniz, bu cihaza girin ve şifrenizin bulunduğu dosyayı silin. Dosyayı sildikten sonra USB'nize sağ tıklayın (Explorer penceresinde) ve Format'ı seçin. USB'niz böylelikle formatlanır. Bu işlem şifrenizden kalan tüm izleri silecektir. Hızlı Format (Quick Format) seçeneğini sakın seçmeyin. Hızlı format veriyi tam anlamıyla güvenli biçimde silmez (24).

TEMEL KULLANMAK VE AYARLAMAK

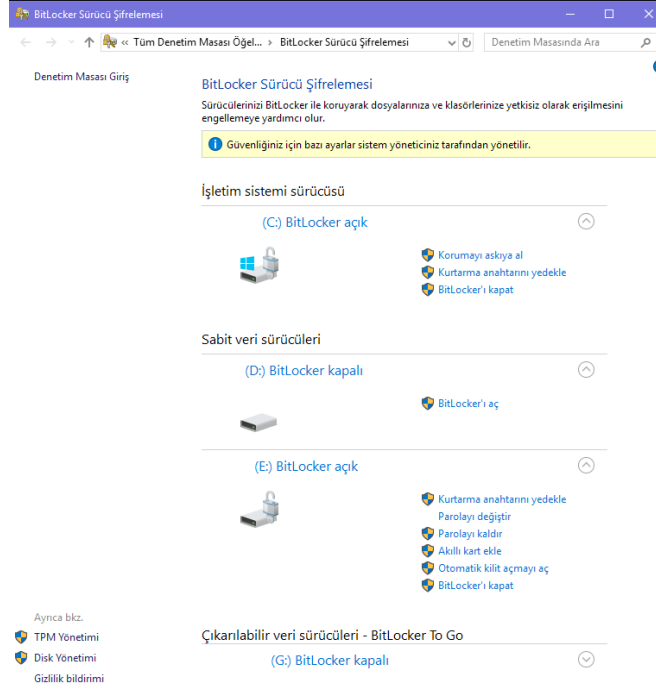
BitLocker menüsünde şifrelemenin aktif olduğunu görüyorsanız, bir kaç seçeneği de göreceksiniz. Elbette bir disk için BitLocker'ı Kapat'abilirsiniz. Ayrıca cihazın Otomatik aç'ılıp (Automatic unlock) açılmayacağına da karar verebilirsiniz. Otomatik açılma, bilgisayarınız başladığında İşletim Sistemi'ne dahil olmayan sabit disklerde, USB'lerde vb. de sizden şifre veya PIN istenmesi anlamına gelir (veya bir USB veya harici diski cihazınıza ilk kez



24

bağladığınızda şifre sorulur). Eğer bu açık değilse BitLocker, Explorer penceresinde görünen diskleri siz onlara tıklayana kadar açmaz (unlock). Sizin isteğinizle açıldığında da sizden şifre veya PİN ister.

Bu otomatik açma özelliği, İşletim Sistemi'nin bulunduğu sabit disklerde uygulanmaz. Bu gibi diskler için bilgisayarınız başlattığınız her seferde sizden şifre veya PİN istenir. Girmedığınız durumda İşletim Sistemi bilgisayarınıza yüklenemez. 25 bazı farklı seçenekleri göstermektedir.



25

Bir diski açtığınızda, bilgisayarınızı kapatana kadar bu disk kilidi açık şekilde duracaktır.

Şimdi temel şifrelemeyi bilgisayarınızda etkinleştirmeyi bitirdiniz.

TEKNİK ÇÖZÜM: GELİŞMİŞ ŞİFRELEME

Gizli şifreleme yaratmak için, VeraCrypt isimli programı indirip yüklemeniz gerekmektedir.

- Veracrypt: <https://veracrypt.codeplex.com/wikipage?title=Downloads>

VeraCrypt'i ister bilgisayarınıza, ister bir USB'ye yükleyebilirsiniz. USB'ye yüklemek daha güvenlidir fakat dosyalarınızı görebilmek için USB'nizin bilgisayarınıza takılı olması gerekir. Hep hatırlattığımız gibi önemli olan dosyayı masaüstünüze değil, yükleyeceğiniz kısıma (USB, sabit disk vb.) doğrudan indirmenizdir.

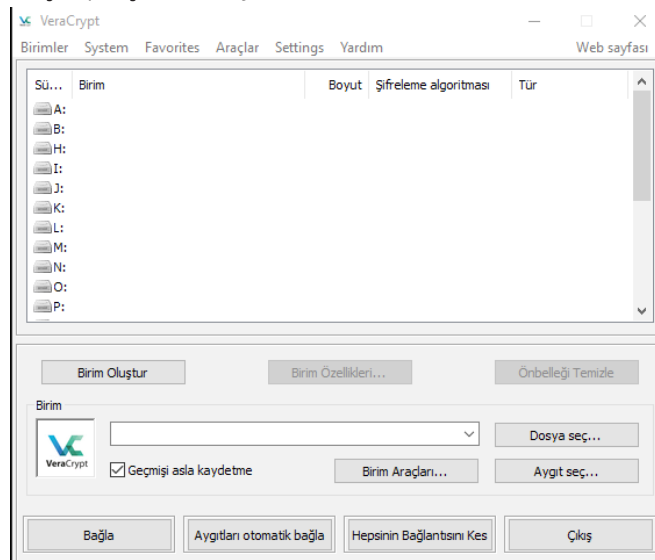
Temel Şifreleme'nin aksine gizli şifreleme kullanmak istediğinizde (örneğin yeni bir dosya indirmeniz gerektiğinde veya belgeleriniz üzerinde çalışmak istediğinizde), VeraCrypt'i başlatıp gizli şifrelemenizi yüklemeniz gerekir. Bu durumda gizli şifrelenen bölüm Explorer'ınızda veya Arama pencerenizde herhangi bir sabit disk veya USB gibi görünecektir. Şifrelenmiş belleğinin yüklenmesi için kullanılan terim tak'tır (mount). Bu belleği çıkarmak/kilitlemek için kullanılan terimse kaldır'dır (dismount). Şifrelenmiş alana çoğunlukla disk bölümü (volume) denir. Bu bölümün geri kalanında bu terimleri sıklıkla kullanacağız. Şifrelenmiş alanı tak'tığınızda bu alan tıpkı bir sabit disk gibi görünecektir (örneğin E: Sürücü İsmi). Kaldır'dığınızdaysa aynı alan gözden kaybolacaktır.

KURULUM

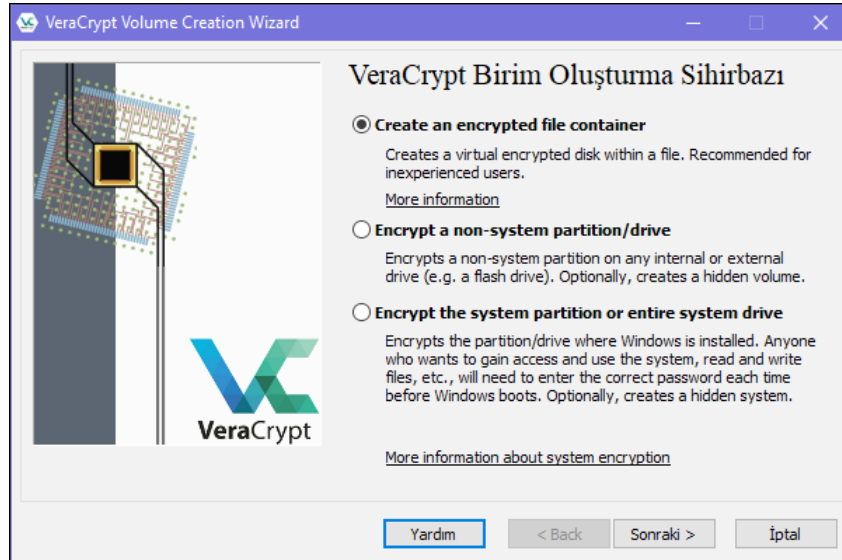
İlk önce bu şifrelemenin nerede konulacağına karar vermeniz gerekir. Bir USB mi kullanmak istiyorsunuz? Sabit bir diskin tamamını mı, bir kısmını mı yoksa ufak bir bölümünü mü kullanacaksınız? Size bu işlemin nasıl yapıldığına size hem bir USB için, hem de bir sabit disk için ayrı ayrı göstereceğiz (Not: İşletim Sisteminizin yüklü olduğu sürücü için bu özelliği kullanmayacağız).

Adım adım yapmanız gerekenler aşağıdadır. Programı yüklemek istediğiniz bölüme yükledikten sonra programı başlatın.

Gördüğünüz ilk pencere, normal kullanımın (mount ve dismount) ana penceresidir (26). Create Volume (Disk Bölümü Oluştur) tuşuna tıklayın.

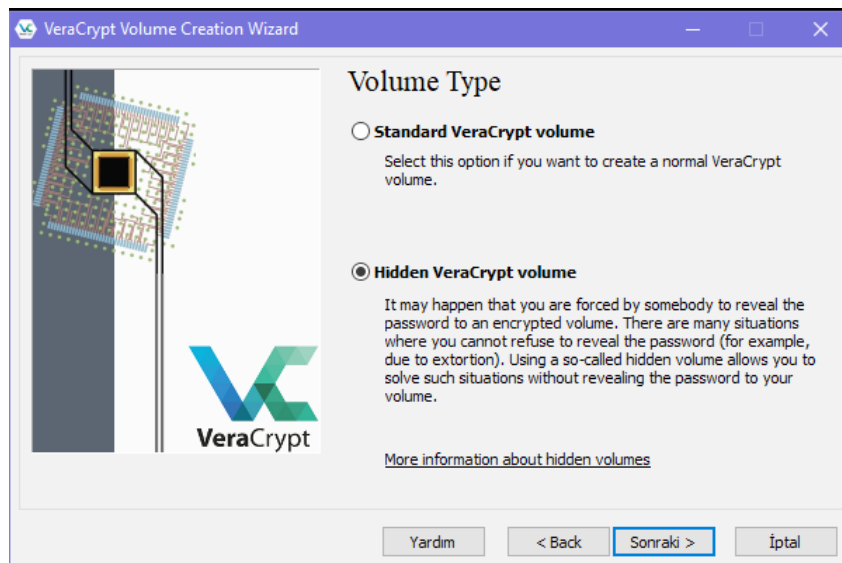


Create Volume'a tıkladıktan sonra iki seçeneğiniz bulunmaktadır (27) (Win10'da sistem ayırma için üçüncü bir seçenek de gösterilmiştir, fakat bunla çok bir işimiz olmayacak). İlk seçenek (ve aynı zamanda da kullanımı en kolay olan) Encrypt a non-system partition/drive (Sisteme ait olmayan bir kısmı/sürücüyü şifrele) olacaktır. Bu seçenek sabit diskinizin tamamını veya bir bölümünü şifreler (İşletim sisteminizin bulunduğu diskiniz için bunu yapamazsınız). Ayrıca harici diskler ve USB'ler için de aynı işlemi gerçekleştirebilir.



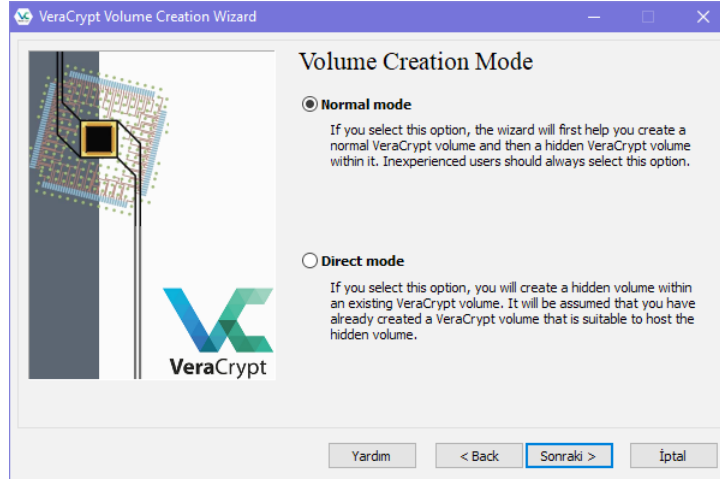
27.

Diğer seçenekte Create an encrypted file container (Şifrelenmiş bir dosya konteynırı oluştur) olacaktır. Burada sabit diskinizin, USB'nizin vb. ne kadarının şifreleneceğine siz kendiniz karar verirsiniz. Bu özelliği kullanmak istiyorsanız, sabit diskinizde veya USB'nizde bir dosya yaratmanız gerekmektedir. Word belgesi veya text dosyası olmayan herhangi tipte bir dosya yaratın; örneğin bir veritabanı dosyası veya bir powerpoint sunumu işinizi görecektir. Bu dosya ileride şifrelenmiş alanı içerisinde tutacaktır. Bu dosyayı silerseniz, içerisinde şifreleyeceğiniz her şeyi de silmiş olursunuz! Açtığınız dosyayı sakın unutmayın ve yanlışlıkla silmeyeceğinizden emin olun.



28

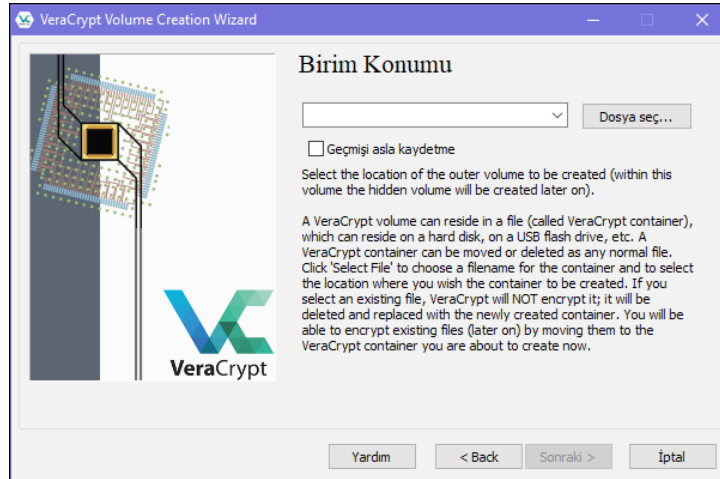
Bu iki seçenektan birini seçtikten sonra Next tuşuna basmanız durumunda, size bir Standart Veracrypt volume (Standart Veracrypt disk bölümü) mu, yoksa Hidden Veracrypt volume (Gizli Veracrypt disk bölümü) mu yaratmak istediğiniz sorulacaktır (28). Hidden (Gizli) olanı seçin ve Next tuşuna tıklayın. Bunun ardından Normal Mode (Normal Mod) veya Direct Mode (Doğrudan Mod) arasında bir seçim yapmanız gerekecektir. Normal Mode'u seçin (Direct Mode daha önceden şifrelenmiş bir alana zaten sahipseniz kullanabileceğiniz bir seçenektir) (29).



29

Buradan sonra göreceğiniz pencere, az önce yaptığınız seçime göre değişecektir

Veracrypt'e geri dönün ve penceredeki Select File (Dosya Seç) tuşuna tıklayın (30). Şifreleme için yarattığınız dosyayı bulun ve seçin. Gelen pencere sizi, dosya içerisinde bulunan tüm verilerin silineceği konusunda uyaracaktır. Bunu kabul edin ('Yes' tuşuna tıklayarak).

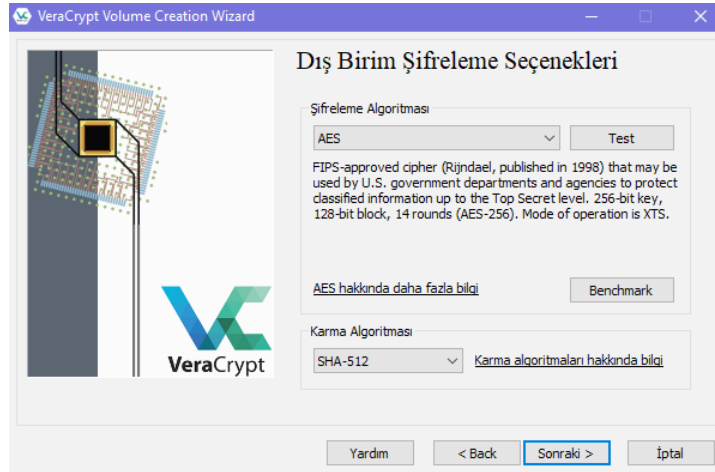


30

Eğer Encrypt a non-system partition/drive'ı seçtiyseniz, Select File tuşuna da tıklayacaksınız ve yeni gelen pencerede hangi USB'nin, sabit diskin veya harici diskin şifrelenmesini istiyorsanız, o cihazı seçeceksiniz. Bu şifreleme işlemi cihaz üzerindeki tüm veriyi silecektir, dolayısıyla cihazda bulunan ve korumak istediğiniz tüm verileri başka bir yere aldığınızdan emin olun.

Bu seçimin ardından geri kalan süreç, iki yöntem için de aynıdır.

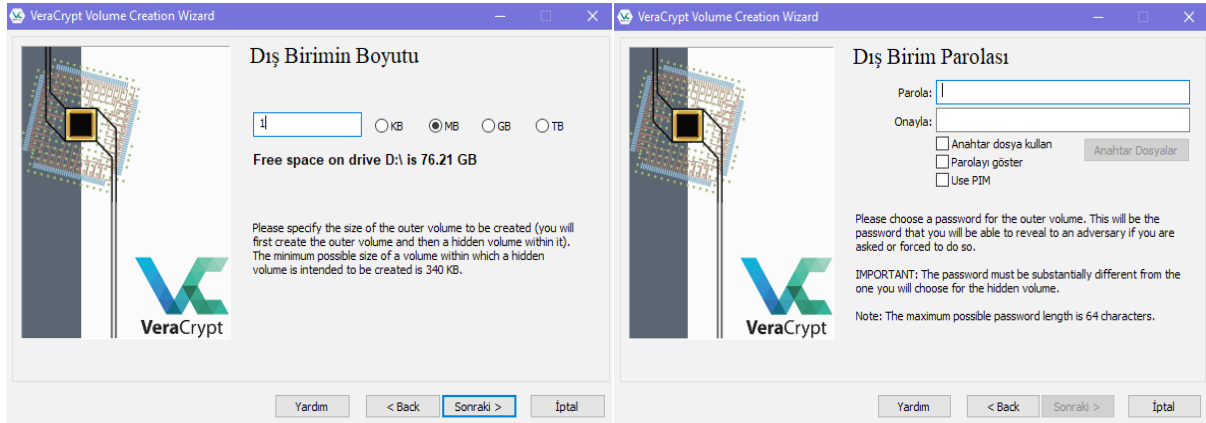
Program öncelikle bir Outer (Dış) disk bölümü yaratacaktır. Bir sonraki adımda herhangi bir değişiklik yapmanıza gerek yoktur (Encryption options – Şifreleme seçenekleri) (31)



31

Sonraki pencere size boyut hakkında sorular soracaktır. Eğer Encrypt a non-system partition/ drive'ı seçtiyseniz bunu değiştiremezsiniz zira tüm bölüm şifrelenecektir. Eğer Create a file container'ı seçtiyseniz, bu bölümün ne boyutta olmasını istediğinizi size soracaktır. Video editlemek gibi çok fazla medya dosyası üzerinde çalışmıyorsanız, 10 GB size yetecektir (32). Seçiminizi yapın ve Next tuşuna tıklayın.

Bir sonraki pencerede Outer (Dış) disk bölümü için bir şifre oluşturacaksınız (33). Bu yem (decoy) olarak kullanacağımız şifrelenen bölümdür ve şifrenin çok gelişmiş olmasına ihtiyaç duymaz. Kolaylıkla hatırlayabileceğiniz bir şifre seçin.



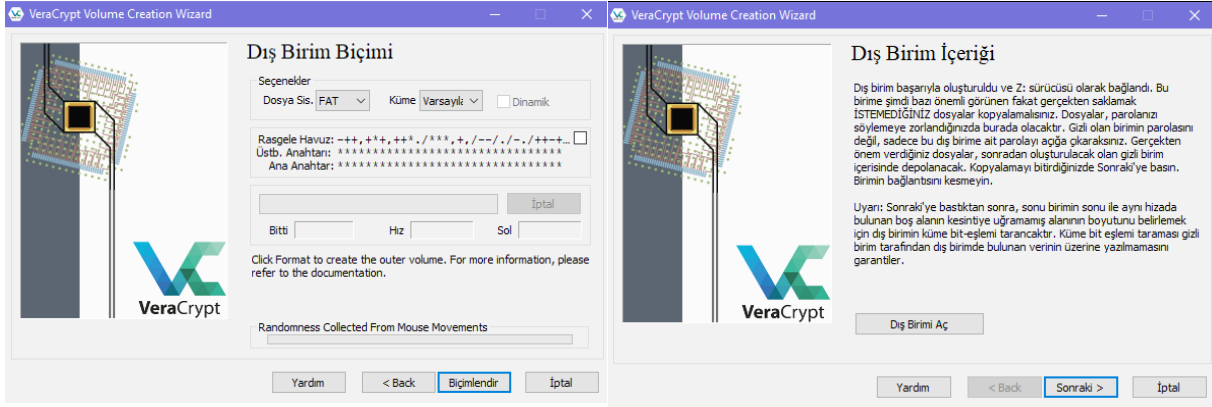
32

33

Bir sonraki pencereye geçtiğinizde şifrelemenin hazırlanma süreci başlayacaktır. Bu süreç, boyuta bağlı olarak değişse dahi çok uzun sürmeyecektir. İşlem boyunca fareyi mümkün olduğunca çok hareket ettirin (34). Bu eylem şifrelemeyi güçlendirecektir. İşlem tamamlandı ve hazır olduğunda, Format tuşuna tıklayın.

Tamamlandıktan sonra size aşağıdaki pencereyi gösterecektir. Next tuşuna tıklayın (35).

Bu işlemin tamamlanmasının ardından Inner (İç) bölümün oluşturulması başlar. Next'e tıklayın. Bu aynı süreci bu kez Inner (İç) bölüm için tekrardan başlatacaktır. Değiştirmeniz gereken tek şey boyut olacaktır ve bunun Dış (Outer) katmanınızdan daha küçük olması gerekmektedir (dış



34

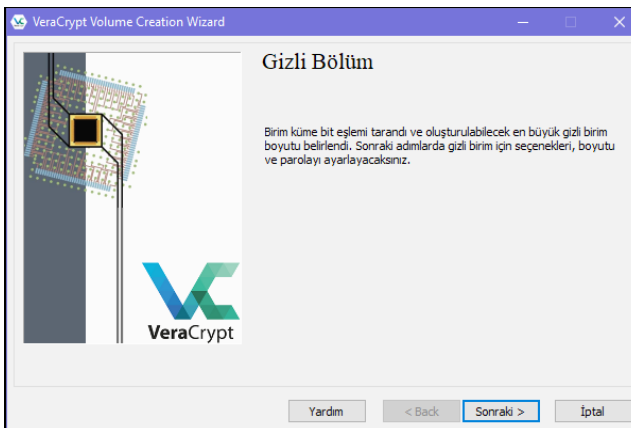
katmanın yarısını seçmenizi öneriyoruz). Bu disk bölümünün ayrıca çok güçlü bir şifreye sahip olması önemlidir. Şifrenizi sakın unutmayın: Unuttuğunuz takdirde bu kısma erişimi sonsuz kadar kaybedeceksiniz. Kalan bütün adımlarsa aynıdır ve tamamlandıklarında karşınıza aşağıdaki pencere çıkacaktır. Exit (Çıkış) tuşuna tıklayın (36).

Tebrikler! Hem Dış hem de İç disk bölümlerinizi artık hazır hale getirdiniz.

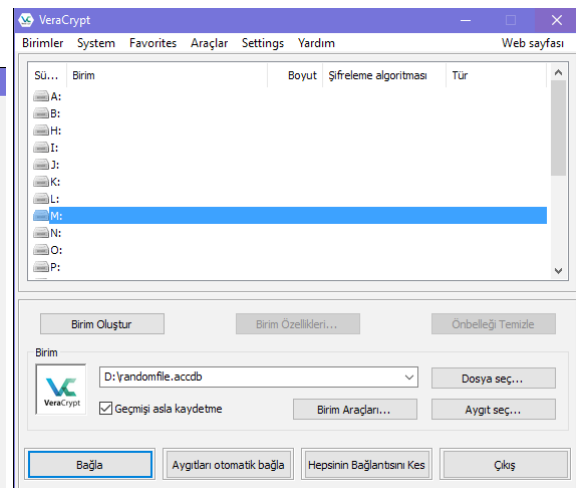
VERACRYPT'İ KULLANMAK

Artık her şeyi kurdunuz ve bunlarla tekrar uğraşmanız ileride gerekmeyecektir. Veracrypt'i kullanmak için programı başlatın (37). Cihazınızı tak'mak (mount) için iki yola sahipsiniz. Önce herhangi bir sürücü adı'na (drive letters) tıklayın. Takıldıktan sonra şifrelenmiş disk bölümü Explorer'da veya Arama pencerenizde bir sabit disk olarak aynı isimle görünecektir. E: veya F: veya tercih ettiğiniz herhangi bir ismi seçin.

Eğer tüm bir sabit diski veya USB'yi şifrelediyseniz, Select Device (Cihaz Seç) tuşuna tıklayın ve önünüze gelen pencereden sabit diski veya USB'yi seçin. Gösterilen şifre kutusuna şifrenizi girin. Daha basit olan şifre otomatikman Dış (Outer) katmanı açacaktır. Daha gelişkin şifreyse İç (Inner) katmanı. Eğer şifrelenmiş alana erişmeleri için başkaları tarafından zorlanırsanız, Dış (Outer) katmanın şifresini kullanın.



36



37

Eğer bir dosya konteynırı seçtiyseniz, Select File (Dosya Seç) tuşuna tıklayın ve şifrenmesi için oluşturduğunuz dosyayı bulun ve seçin. Aynı şekilde daha basit olan şifrenizi girerseniz Dış (Outer) katman, daha gelişkin şifrenizi girerseniz İç (Inner) katmanı açarsınız.

Burada ayrıca bir Auto-mount Devices (Cihazları otomatikman tak) tuşu bulunmaktadır. Buna tıkladığınızda takılabilir cihazlar otomatik olarak bulunacak ve bunlara dair şifreler sizden istenecektir. Bunun devamındaki süreç aynı şekilde işler; basit şifreniz Dış (Outer) katmanı, gelişkin şifreniz İç (Inner) katmanı açacaktır. Ne yazık ki Auto-mount işlemi her zaman çalışmaz ve yüklemek için biraz daha uzun bir süre alır. Fakat çalışıyorsa, şifrelenmiş disk bölümlerinize ulaşmak için en kolay yol budur.

Disk bölümünüzü taktığınızda, programı kapatıp çalışmaya başlayabilirsiniz.

İşinizi bitirdiğinizde ve çalışma dosyalarınıza erişmeye daha fazla ihtiyacınız kalmadığında, veya bilgisayarınızın başından ayrılacağınız zaman, programı tekrar başlatın ve Dismount all (Hepsini kaldır) tuşuna tıklayın. Bu işlem, takılı olan tüm şifrelenmiş diskleri kapatır (ve bu diskler Explorer veya Arama penceresinde artık görünmez).

İleride yapmanız gereken tek şey tak (mount) ve kaldır (dismount) olacaktır.

SON ADIMLAR

Gerçek gizli şifrelemenize (İç katman) ulaşımı engelleme yeteneğinize İngilizce plausible deniability denir; hukuki olarak bu kavram gerçekçi inkar olarak çevrilebilir ve bu kavram kendinizi korumanızın anahtarıdır. Fakat bu kavramın işleyebilmesi için inandırıcı olması gerekmektedir. İnandırıcıdan kastımız, Dış katmanda Yem olarak kullandığınız bilginin, paylaşmak istemeyeceğiniz bilgiler olması gerekmektedir. Başkaları tarafından Dış katmanınızı açmaya zorlandığınızda ve bu katmanı açtığınızda bu kişilerin, eriştikleri bilginin tarafınızca saklanmaya çalışan bir bilgi olduğuna inanmaları gerekmektedir. Eğer bu katman boşsa veya sadece müzik vb. manasız dosyalar bulunduruyorsa, bu kişiler muhtemelen sakladığınız şeyin bu olmadığını anlayacak ve sizden asıl kaynağı almaya çalışacaklardır.

Bu nedenle kurulumdan sonra, Dış katmanınıza neler koyacağınız konusunda biraz düşünün: Buraya yerleştireceğiniz dosyaların hassas olması, fakat çok çok hassas olmaması önemlidir. Buradaki bilginin “hassas görünümlü” olması gerekmektedir. Örneğin buraya bazı önemli banka dökümanlarını, korsan medya dosyalarını veya karalisteli kitapları/pdf'leri koyabilirsiniz. İnandırıcılık adına buraya bazı çalışma dosyalarını da koymalısınız; örneğin raporlar, yazdığınız belgeler veya indirdiğiniz işle alakalı dosyalar. Artık işinize yaramayacak, üzerinde çalışmayacağınız ve en önemlisi gerçekten hassas bilgileri içermeyen bu iş dosyalarını buraya yerleştirmeniz, Dış katmanınızı daha inandırıcı kılacaktır. Bu dosyaları arada bir güncellemeyi, yanlarına yeni dosyalar eklemeyi ihmal etmeyin; böylelikle Dış katmanınızın inandırıcılığını korumaya devam edebilirsiniz.

Eğer ilerleyen zamanda güvenlik kaygılarınız artarsa, Dış katmana bir kaç yeni çalışma dosyanızı daha kopyalayın. Fakat unutmayın: Asıl hassas dosyalarınız asla buraya girmemelidir. Bu bölümün bir Yem olduğunu aklınızdan çıkarmayın. Bu Yem'in tek amacı, başkalarının asıl

bilgilerinize/dosyalarınıza erişimini engellemek ve arama sürecinde üçüncü kişileri başınızdan savmaktır.

Dış katmanınızı güncellemedeki temel sebep, buraya aktarılan dosyaların, değiştirilen verilen vb. bazen bir zaman damgasına (time stamp) sahip olmasıdır. Eğer Dış katmanınıza erişim sağlanır ve buradaki dosyaların iki yıldan beri hiç değiştirilmediği farkedilirse, bu bölümü aslında hiç kullanmadığınız ortaya çıkabilir, yeminiz “yutulmayabilir” ve İç katmanınız varolduğuna dair şüpheler ortaya çıkabilir.

Bu sistemi oluşturmanın en kolay yolu tüm çalışma dosyalarınız İç katmana aktarmaktır. Ardından bu dosyaların üzerinden geçip bir kısmını Dış katmana kopyalayabilirsiniz. Unutmayın: Dış katmana aktaracağınız dosyalar işinizle alakalı olmalıdır, fakat hassas veriler, isim/detay içeren dosyalar ve başkalarına zarar vermek için kullanılacak bilgiler olmamalıdır.

Dış katmanın inandırıcı olması gerektiğinden, bu katmana ayrıca hassas veya kişisel sayılabilecek başka dosyaları da eklemenizi öneriyoruz. Örnek olarak aşağıdaki maddeleri gözden geçirin:

Kısaca Dış katman, normal koşullarda güvenli olacaktır ve üçüncü kişilerin sizden şifrelerinizi temin etmeye çalıştığı durumlardaysa bir Yem görevi görecektir. Hazırlıklı olmanız gereken şey Dış katmana başkalarının eriştiği durumda kişisel bilgilerinizin görüleceği ve okunacağıdır. Ama asıl önemli olan şey bu kişileri, eriştikleri bilgilerin tarafınızca “korunmaya” çalışılan bilgiler olduğuna ikna etmenizdir.

İnandırıcı olmak için Dış katmanın şifresini hemen veya kolaylıkla vermeyin. Sorulduğu durumlarda direnmeye devam etmelisiniz; aksi takdirde buraya erişmeye çalışan kişiler bundan şüphelenebilir. Eğer size inanırlarsa, çok büyük ihtimalle asıl hassas bilgileriniz korunacaktır. Ve evet; başkalarının bu Dış katmandaki bilgilere ulaşması çok nahoş olabilir. Fakat bu durumu yaşayabileceğiniz olası tehlikeli sonuçlarla karşılaştırdığınızda, yapacağınız seçim fazlasıyla basittir. Hatta yukarıda örneklendirmeye çalıştığımız biçimde kişisel bilgilere, verilere, fotoğraflara vb. sahip değilseniz, bu gibi dosyaları (sahte dahi olsa) oluşturmanızı ve buraya yerleştirmenizi öneriyoruz. Bu hazırlık, emin olun yaşayabileceğiniz sonuçlar açısından çok ciddi farklara yol açacaktır.

PRATİK DİJİTAL GÜVENLİK

ALT BÖLÜM 6 BİLGİYİ PAYLAŞMA



Bir çok kişi için e-posta aracılığıyla güvenli iletişim kritik bir meseledir. Bu bölüm e-postaların güvenli kullanımının nasıl kolaylıkla yapılabileceğini ve ciddi bir tehditle karşı karşıya kaldığınızda e-postanızı nasıl kendinizi koruyacak şekilde kullanabileceğinizi gösterecektir.

Bu bölüm temel olarak e-postayla ilgilenecektir. Sohbet programlarına (Chatting), SMS'e ve mobil telefonla iletişime, Bölüm 11: Güvenli Uygulamalar bölümünde değinilecektir. Bu bölüm ayrıca özellikle otomatik olarak şifrelendirilmiş web-mail'lerin kolay kullanımına dair seçeneklere odaklanarak, e-posta şifrelemeye de (encryption) değinecektir.

Şifreleme işe yarayan bir kavramdır, fakat günlük meseleler için fazlasıyla karmaşık hale gelebilir. Bu nedenle bu bölüm PGP şifrelemeye dair bilgi içermemektedir.

Çalınma veya zor yoluyla e-posta şifrenize ulaşıldığında şifrelemenin hiçbir türü size koruyamayacaktır. Şifreleme, takım çantanızdaki aletlerden yalnızca biridir; çevrimiçi ve çevrimdışı güvenliğinizi yükseltmek için başka davranışlarla birleştirilerek kullanılmalıdır.

Önceki bölümlerde de değindiğimiz üzere güvenliğinizi yükseltmede, çalışmalarınız için kullandığınız tarayıcınızı (browser) nasıl kullandığınız çok büyük bir rol oynamaktadır; kötü niyetli tarafların hangi e-posta hizmetini kullandığınızı öğrenmesi güçleşecektir. Boş Gelen Kutusu Politikası'nı olabildiğince denemeyi ve kullanmayı unutmayın; bunu uygulamaya geçirdiğiniz durumda, şifrenizi ele geçirmiş biri e-postanızda hassas hiçbir şeye ulaşamayacaktır.

“UÇTAN UÇA FARKI

Bu iki kavramın anlaşılması elzemdir.

'Normal' şifreleme kullandığınız hizmetin (örn. Gmail) verilerinizi (örn. mail) şifrelediği anlamına gelmektedir. Bunun anlamı bir e-postayı gönderdiğinizde bunun önce Google'ın sunucularına ulaşip, burada şifrelenip, ardından gönderdiğiniz alıcıya iletilmesidir. Burada iki problem mevcuttur. İlki, İnternet Hizmet Sağlayıcı'nızın Google'a gönderdiğiniz veriyi okuyabilme ihtimaline sahip olmasıdır (eğer VPN veya TOR kullanmıyorsanız). İkincisi, hizmet sağlayıcınızın (Google) verilerinizin şifrelenmesi noktasında tam yetkiye sahip olmasıdır. Bunun anlamı aynı kurumun istediği takdirde verilerinizin şifresini çözme (decryption) yetkisine de sahip olmasıdır. Diyelim Google'a bu konuda güveniniz tam. Yine de kullandığınız başka

e-posta sağlayıcılarına dair güveninizi gözden geçirmeniz gerekebilir. Zira bu kurumlar güçlü aktörlerce zorlandıklarında, size özel verilerin şifresini çözmek noktasında çok direngen olamayabilirler. Genel olarak kamusallaşmasını istemediğiniz her türlü iletişim için her zaman uçtan uça şifreleme kullanmalısınız.

Uçtan uça şifreleme, verinin kaynağından itibaren şifrelendiği anlamına gelir (örn. Bilgisayarınızda veya telefonunuzda). Ardından bu veri alıcıya iletilir ve aynı veri alıcının bilgisayarında şifre çözümüne uğratılır. Bunun anlamı İnternet Hizmet Sağlayıcı'nızın sizi gözetleyemeyeceği ve iletişim hizmetini sağlayan kurumun da verilerinizin neyi içerdiğini bilemeyeceğidir (örn. Mesajlar, e-postalar vb.). Uçtan uça şifreleme önemli bir meseledir ve bir seçenek olarak mevcut olduğu her durumda kullanılmalıdır. Bu durumda hizmet sağlayan herhangi bir şirket sizi gözetlemek istese veya verilerinizi başkalarına vermeye zorlansa dahi bunu yapamazlar; çünkü haberleşmelerinizi bu şirket şifrelemediği için, şifre çözümüne uğratması da mümkün değildir.

E-POSTA KULLANIMI

Güvenlik ve teknoloji uzmanları sizi PGP kullanmaya teşvik edeceklerdir fakat PGP'yi ayarlamak bazen kafa karıştırıcı olabilir ve bazı insanlar PGP'nin kullanımını külfetli bulmaktadırlar. Örneğin Türkiye'deki bir çok gazeteci ve STK çalışanı, - daha önceden dijital güvenlik eğitimlerine katılmış olsalar dahi, PGP uygulamalarından birinin arayüzünden memnun kalmadıklarını veya PGP'nin zamanlarını çok tükettiğini farkedip kullanmayı bıraktıklarını (haliyle de eski ve güvenlik seviyesi daha düşük iletişim biçimlerine geri döndüklerini) belirtmektedir. Biz bundan kaçınmak istiyoruz. PGP kullanımında kendinizi rahat hissediyor olabilirsiniz, ne mutlu size! Eğer öyleyse, bu konuya ileride değineceğiz. Şimdilik bir çok kişinin güvenli, fakat pratik ve sürdürülebilir bir çözümden yana olduğunu düşündüğümüzden, aşağıdaki bölüm güvenli webmail sistemlerinden bahsedecektir.

Uçtan uça şifreleme sağlayan ve sunucuları Türkiye'nin dışında bulunan bir webmail seçin.

Bilgisayarınızda (veya telefonunuzda) bu e-postalara erişim için kullanılan uygulamalardan kaçınmalı, e-postanıza yalnızca çalışmalarınız için kullandığınız tarayıcınızdan girmelisiniz. Bilgisayarınızda ayrıca bir e-posta okuyucu (mail client) kullanmaktan da kaçınmalısınız. E-posta okuyuculara örnek olarak Mozilla tarafından (aynı zamanda Firefox'un da tasarımcısı) geliştirilmiş Thunderbird verilebilir ve bu okuyucu PGP'nin kurulumunu anlatmak için sıkça kullanılır. Başka örnekler olara Microsoft Outlook ve Opera Mail de verilebilir.

Güvenli bir webmail hazırlarken, e-posta adresinizin isim kısmında kendi adınızı veya çok bilinen bir lakabınızı kullanmayın. Bu sadece başkalarının hangi e-posta adreslerinin size ait olduğunu bulmasını kolaylaştırır.

Uçtan uca şifreleme kullanan güvenli webmail sistemleri mevcuttur. Muhtemelen en iyisi, ilave güvenlik seçeneklerine de sahip olan ProtonMail.com'dur. Alternatif olarak Tutanota.com ve Hushmail.com'u da deneyebilirsiniz. Protonmail ve Tutanota'nın arayüzleri hem İngilizce hem de Türkçe mevcutken, Hushmail'in sadece İngilizce sürümü bulunmaktadır.

"Bir çok e-posta sağlayıcı ve şifreleme sistemi 'Konu' başlığını şifrelememektedir. Çoğu şifrelemeli e-postalar kullandığınız başlığı/konuyu olduğu gibi göstermeye devam edecektir. Gerekli durumlarda daha kriptik mail başlıkları kullanmanızı, haberleştiğiniz insanlarla kendi 'kod kelimelerinizi' oluşturmanızı öneririz."

Bu webmail sistemlerinin dezavantajlı yanı, maksimum güvenliği sadece kendi oturumları içerisinde gerçekleştirebiliyor olmalarıdır: Örneğin Protonmail'dan Protonmail'a veya Tutanota'dan Tutanota'ya haberleşirken. Bu nedenle yeni bir güvenli e-posta oluştururken, en sık iletişimde olduğunuz insanlarla, dostlarınızla, iş arkadaşlarınızla, ortaklarınızla vb. bu meseleyi önden konuşmanız iyi olabilir. Bu yolla daha fazla aynı hizmeti kullanabilir, kendi içinizde size ait güvenli bir haberleşme ağını yaratabilirsiniz. Bundan kaçınmanın tek bir yolu vardır fakat bunu bir kuraldan ziyade, bir istisna gibi kabul etmemiz gerekmektedir.

Bu webmail sistemlerinden normal e-postalara güvenli e-posta göndermenin bir yolu vardır; yapmanız gereken alıcıya gönderdiğiniz mail'in şifresini çözebileceği bir şifre göndermek ve böylelikle alıcının gönderdiğiniz mail'i okuyabilmesini sağlamaktır. Şifre çözme işlemini gerçekleştirecek şifre, sadece bu yolla gönderilen tekil e-postalar için işlem görecektir. Bu noktada şifrenizi güvenli yollarla göndermeniz önemlidir; kendi kendini yoketmeye ayarlı Signal veya Telegram mesajları burada size yardımcı olabilir. Bu sistemlere ileride değineceğiz.

ProtonMail'i önermemizin sebebi, kendi kendini yoketme fonksiyonuna sahip e-postalar gönderebilmesinden ötürüdür. Bir zamanlayıcı ayarlayarak gönderdiğiniz e-postanın, sizin 'gönderilen' kutunuzda ve alıcı(lar)ın 'gelen' kutusunda belirli bir süre durup ardından kendi kendini silmesini otomatik olarak silmesini sağlayabilirsiniz. Bu, özellikle e-posta gönderdiğiniz insanların iyi bir güvenlik protokolünü takip etmediği veya böyle detayları gözden kaçırabileceği durumlarda işinize yarayabilir. Bu şekilde bilginin güvenliğini, ama daha da önemlisi bilginin içerdiği insanların güvenliğini sağlama alabilirsiniz. ProtonMail'in bu özelliği, Boş Gelen Kutusu Politikası'nı hayata geçirmenizi kolaylaştırabilir.

Bu webmail'ler ayrıca bir cep telefonu uygulaması da tahsis etmektedirler. Fakat bunu sizin için güvenli bir karar olup olmadığına siz karar vermelisiniz. Bu, e-postanıza telefonunuzdan mobil olarak erişebilmenizi sağlarken, aynı zamanda telefonunuza bakan birinin bu e-posta hizmetlerinden hangilerini kullandığınızı anlamasına da sebep olabilir. Kötü niyetli taraflar doğrudan ProtonMail şifrenizi sizden almaya çalışmayabilirler, hatta belki bu hizmeti kullandığınızı bile bilmeyebilirler. Fakat uygulamayı telefonunuzda gördüklerinde bu fikirleri değiştirebilir. Ayrıca uygulamayı PIN kodu veya şifresi olmayan bir telefonda kullanıyorsanız veya uygulamada oturumunuz sürekli açıksa, bu ek bir güvenlik zaafı teşkil edecektir. Oturumunuzun sürekli açık olması, telefonunuzu ele geçiren birinin doğrudan gelen kutunuzu görebileceği, mail'lerinizi okuyabileceği ve hatta e-postanızdaki kişilere yönelik zarar verici mail'ler gönderebileceği anlamına gelir. Bu durumun dayanışma ağınıza, sivil toplum kuruluşunuza veya gazetecilerin kendi aralarında kullandığı bir haberleşme ağına vereceği zararı hayal etmeye çalışın. Uygulamalara dair tehlikeler bu kılavuzun Bölüm III: Telefon Güvenliği kısmında daha detaylı olarak anlatılmaktadır.

Bu e-postalardan birini kurduğunuzda, doğrudan ayarlar bölümüne gidin ve sistemin ayarlarını anlamaya çalışın. Başlarken herhangi bir özel değişiklik yapmanıza lüzum yoktur zira bu sistemler başlangıçlarında en yüksek güvenlik seviyesiyle birlikte gelirler. Teknik Çözüm: ProtonMail Kullanımı kısmında ProtonMail'in arayüzüne dair daha fazla bilgi bulabilir ve diğer "normal" e-postalarla nasıl güvenli haberleşebileceğinizi, bunlara nasıl kendi kendini yokeden mesajlar gönderebileceğinizi öğrenebilirsiniz.

IMAP VE E-POSTA OKUYUCULAR

Güvenli e-postanız için Outlook, Mail veya Thunderbird gibi e-posta okuyuculardan kaçınmanızı öneriyoruz. Bahsettiğimiz güvenli e-postalar hali hazırda bu e-posta okuyucuları zaten desteklememektedir. Fakat asıl önemli husus bu okuyuculara bir PIN kodu veya şifre yoluyla erişimi engellemenin güvenilir bir yolunun olmamasıdır (varolan yöntemlerde bug'lar mevcuttur, bu nedenle güvenli kabul edilmemektedirler). Bu

durum sizin için gereksiz bir güvenlik riski taşır ve Boş Gelen Kutusu Politikası kullandığınız takdirde kullanışlı değillerdir. Telefonunuzda veya bilgisayarınızda bir e-posta programının kurulu olması, bu cihazlarınıza erişim sağlamış kişilerin hangi hizmeti kullandığınızı öğrenmesine ve istedikleri takdirde bu hizmetler için kullandığınız şifreleri sizden edinmeye çalışmalarına neden olabilir. Bilgisayarınızda veya telefonunuzda bir e-posta okuyucunun bulunması, buraya kadar tartıştığımız anahtar meselelerin çoğuyla çelişir – özellikle de gizliliğinizi ve kullandığınız hizmetin ne olduğunu saklama noktasında.

4 ANAHTAR DAVRANIŞI HATIRLAYALIM

BOŞ GELEN KUTUSU

E-postanıza erişileceğini varsayın. Boş Gelen Kutusu Politikası okunacak hiçbir şey olmayacağını garantiler. Kısaca gelen kutunuzu olabildiğince boş bırakın. Çoğu zaman bu işlem hiçbir problem arz etmeyecek, zira büyük ihtimalle çoğu yazışmanızı saklamaya ihtiyaç duymuyorsunuz. Bunun önemini ne kadar anlatsak az. Bu politikayı iş arkadaşlarınız veya dostlarınızın da uyguladığından emin olun.

CEVAPLAMAMA ANLAŞMASI

Aldığınız her e-posta için bunu izlemeniz şart değildir. Fakat özellikle hassas veya önemli mesajlar için (örneğin içerisinde spesifik isimler, tarihler, konular veya bilgiler barındıran, içerdiği kişiler için gelecekte risk arz edebilecek konular içeren e-postalar) bunu uygulamanız daha iyi olabilir.

Çoğunlukla yazışırken yeni bir e-posta yazmaktansa var olan bir e-postayı 'cevaplarız'. Bu sayede aynı e-postada geçmişteki yazışmalar da görünür. Bu yazışmalar çok uzun bir zamana yayılır ve bu nedenle ufak bir yeni cevap, uzun bir geçmişi barındırıyor olabilir.

Cevapla fonksiyonundan olabildiğince uzak durun. Kullandığınız takdirde, orijinal metni silin. Bu alışkanlığınızın süresi içinde olabildiğince az bilgiye erişilebilmesi demek.

OTURUM AÇMAKTAN KAÇINMAK VE CROSS SERVICE LOGIN DANGER

Otomatik oturum açmak gerçek bir tehdittir. Özellikle de aynı sağlayıcının bir oturumunu açmak çoğunlukla o sağlayıcıya ait bir çok oturumun da açılması anlamına geldiği için. Örneğin tarayıcınızda Gmail oturumunuzu açtığınızda, otomatik olarak Google'a ait diğer bütün hizmetlerde de oturumunuz açılacaktır; örneğin Google Drive (bulut depolama), Youtube vb. Apple, Windows vb. sistemlerin sağladığı benzer hizmetler için de bu geçerlidir.

Bundan kaçınmanın en iyi yolu, herhangi bir firmadan sadece tek bir hizmet kullanmaktır. Eğer Gmail kullanıyorsanız, bulut depolama için Google Drive kullanmayın (benzer örnekler çoğaltılabilir). Bu otomatik oturum açma ve otomatik senkronizasyon tehlikelerinin önüne geçecektir. Çalışmalarınızda kullandığını tarayıcınız için hiçbir oturumunuzu "otomatik" hale getirmeyin. Bu sadece başkalarının size ait diğer hesaplara ulaşma riskini kolaylaştırır.

Günümüzde bu gibi hizmetler otomatik senkronizasyon yapmayı da seviyorlar. Eğer telefonunuzda google Chrome kullanıyorsanız ve PC'nizde/ MAC'inizde Google Chrome'da oturum açarsanız, izin verildiği takdirde otomatik senkronizasyon bu iki farklı cihazdaki iki farklı tarayıcıyı birbiriyle senkronize edecektir. Bilgisayarınızdaki Chrome'da kaydedilmiş olan her türlü yer işareti, geçmiş, kayıtlı şifreler ve dahası bu yolla telefonunuzdaki Chrome'da da görülecektir. Bu, ciddi bir meseledir.

UYGULAMA

Win10 artık tıpkı telefonunuzdaki gibi uygulamaları bilgisayarınıza yüklemenize izin veriyor olsa dahi, uygulamaları (Apps) bilgisayarınızda kullanmaktan kaçınmanızı öneririz. Bilgisayar sürümlerinde bu uygulamaların çoğunun yerleşik (built-in) şifreleri veya PİN kodları yoktur. Bu bilgisayarınıza erişimi olan herkesin uygulamayı açarak mesajlarınızı, e-postalarınızı, takviminizi görebileceği ve hatta sizmiş gibi davranarak başkalarına mesaj gönderebileceği anlamına gelir. Bir uygulamanın cihazınızda yüklü olması ayrıca doğrudan hangi hizmeti kullandığınızı açık eder ve kendinizi koruyabilme kapasitenizi düşürür. Bu uygulamaların bilgisayardaki örnekleri Signal Private Messenger veya WhatsApp masaüstü uygulamalarıdır.

BULUT DEPOLAMA

Bulut depolama çoğunlukla bilgilerinizin internette çevrim içi depolanması anlamına gelir. Bazı bulut hizmetleri katı olarak sadece iş belgelerinizi yedeklemek için kullanılırken, bazılarıysa bilgisayar ayarlarınızı ve programlarınızı depolamak veya güncellemek için vardır. Diğerleriyse bir işbirliği platformu olarak çalışarak başkalarıyla belgelerinizi paylaşmanızı veya aynı anda aynı belge üzerinde çalışmanızı sağlar. Genel olarak internette online depolanan her şey daha güvenliksizdir. Bu nedenle hassas çalışma belgeleriniz/bilgileriniz için asla Windows'un OneDrive'ını, MAC'in iCloud'unu veya Google'ın Drive'ını kullanmayın. Bunları söylemekle birlikte bulut hizmetlerini kullanmak her zaman kötü bir anlama gelmeyebilir; ne yaptığınızı biliyorsanız bunları kullanmanın güvenli yolları da mevcuttur.

Şüphesiz ki –farkında olmasanız dahi, hali hazırda bir bulut depolama servisi kullanıyorsunuz. Örneğin Gmail hesabınız varsa, Google Drive hesabınız da otomatikman vardır. Eğer bir Mac bilgisayarınız varsa aynı şekilde iCloud'a ve eğer bir Windows kullanıyorsanız ya da bir Hotmail hesabınız varsa, OneDrive'a sahipsiniz. Çoğu bulut hizmeti bilgisayarınıza veya cep telefonunuza önceden yüklenmiş şekilde gelir.

Eğer bulut hizmetlerine ihtiyacınız varsa odaklanmanız gereken şey, spesifik olarak seçtiğiniz dosyaları yedekleyebilen bir hizmet kullanıyor olmaktır. Bu programlar bilgisayarınızın veya telefonunuzun arka planında çalışır ve herhangi bir değişiklik yaptığınızda bulut belleği güncellenir. Bilgisayarınızı veya telefonunuzu kaybettiğinizde, çaldırıldığınızda veya bu cihazlara el konulduğu durumlarda bulut, bir yedek işlevi görebilir. Diğer yandan bulutta sakladığınız her şeye başkalarının erişme ihtimali vardır ve bu nedente korunmaları gerekir.

İlkin telefonunuzu ve bilgisayarınızı kontrol etmeli, hangi hizmetlerin cihazlarınızda etkin olduğu ve hangi uygulamaların yüklendiğini görmelisiniz. Kullanmadıklarınızı devre dışı bırakın. Telefonlar, kişisel ayarlarınız haricinde fotoğraflarınızı, videolarınızı ve belgelerinizi otomatik olarak kaydedecek şekilde ayarlanmışlar. Bu sizin için bir tehlike arz edebilir; özellikle de telefonunuzdaki çoğu hizmetin/uygulamanın herhangi bir kullanıcı adı veya şifreye ihtiyaç duymadan kullanılabilir olması. Kullanmayacağınız her türlü bulut hizmetini silin/ortadan kaldırın.

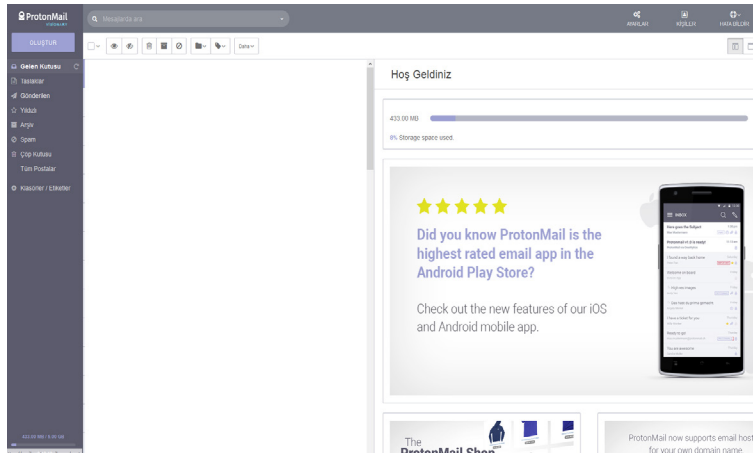
İkincisiyse, bilgilerinizi saklamak hakkında konuştuğumuz bu konulara paralel olarak, uygulamaların bulut belleğinize erişimine güvenmemenizdir. Uygulamaların kullanımı kolaydır fakat aynı zamanda gerçek riskler taşırlar. Telefonunuzu edinen herhangi bir kişi kolaylıkla kullandığınız hizmetleri görebilir, çeşitli yollarla sizden kullanıcı isminizi ve/veya şifrelerinizi almaya çalışabilirler. Çalışma verilerinizi depolamada gizli şifreleme kullanıyor olmanızın, çevrimiçi bulut belleğinizde aynı veriyi korumak için gerekli adımları atmadığınız durumda hiçbir anlamı yoktur. Bulut hizmetlerine sadece çalışma amaçlı kullandığınız tarayıcınız, VPN'niniz aracılığıyla ulaşın. Bir çok seçenek olmasına karşın size SpiderOAK veya Tresorit öneriyoruz. Eğer Bulut depolama yapan bir firma kullanmak istiyorsanız, size uygun seçeneklere sahip olanı google'dan araştırmalısınız.

Bazı bulut hizmetlerinin arkasında yeni belgeleri karşıya yükleyen ve çalıştığınız sırada değişiklikler yapan süreçler yürümektedir. Bunlardan uzak durmaya çalışın. Diğerleri içinse bulut hizmetine sizin girmeniz ve online olarak kaydetmek istediğiniz dosyaları karşıya sizin yüklemeniz gerekir. Sizi daha korunaklı hale getirdiğinden ve cihazınıza erişim sağlamış üçüncü kişilerden hizmet tercihlerinizi sakladığı için bu seçeneği öneriyoruz.

TEKNİK ÇÖZÜM: PROTONMAIL

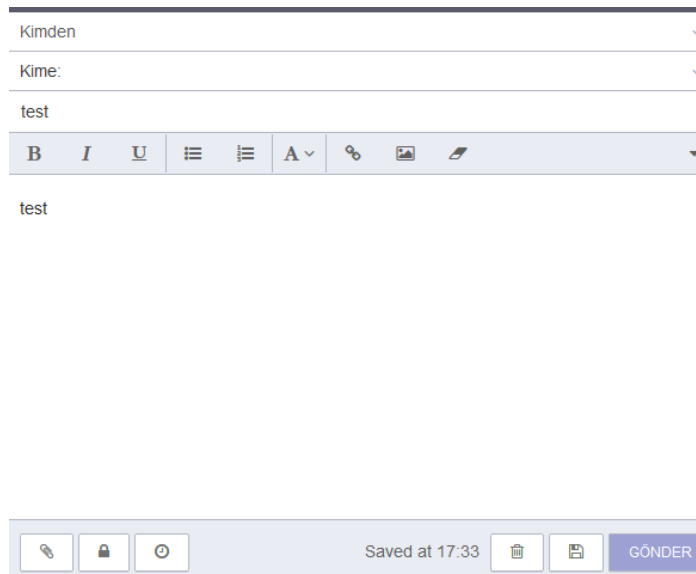
Bu güvenli webmail seçeneklerini kullanmak çok kolaydır ve aslında çok fazla açıklamaya gerek duymamaktadırlar. Fakat dil kısıtlarının varolabileceğini gözeterek, arayüze dair aşağıdaki ekran görüntüleri bir miktar açıklanacaktır. Bunlara çalışın, e-postanıza girin ve etrafa bir bakın; hiç güçlük yaşamadan ProtonMail'i kullanabileceğinize eminiz. Eğer Tutanota veya Hushmail kullanmayı seçtiyseniz, ProtonMail'le neredeyse aynı şekilde çalıştıklarını göreceksiniz.

Eğer ProtonMail'i kullanarak normal bir e-posta adresine mesaj göndermek istiyorsanız (38) (örneğin Gmail), bir şifre seçip yazmalısınız. E-postayı gönderdiğinizde alıcı bir e-posta değil, bir link alacaktır (kendi e-postasının gelen kutusunda). Bu linke tıkladıklarında mesajı okuyabilmeleri (ve cevaplayabilmeleri) için bir şifre girmeleri gerektiğini göreceklidir.



38

Bu nedenle birine e-posta gönderdiğinizde, güvenli bir mesajlaşma uygulaması (chat app) kullanarak karşınızdakine şifreyi ulaştırmanız gerekmektedir. Alternatif olarak sözlü şekilde önceden beraber belirlediğiniz bir şifreyi de kullanabilirsiniz. Şifreyi Signal veya Telegram üzerinden kendi kendini yoketme özelliği etkin bir mesajla göndermenizi öneriyoruz. Bu konuda daha fazla bilgi için KISIM III'ün (Telefon Güvenliği) Bölüm 11: Kullanımı Güvenli Uygulamalar kısmını ziyaret edebilirsiniz.

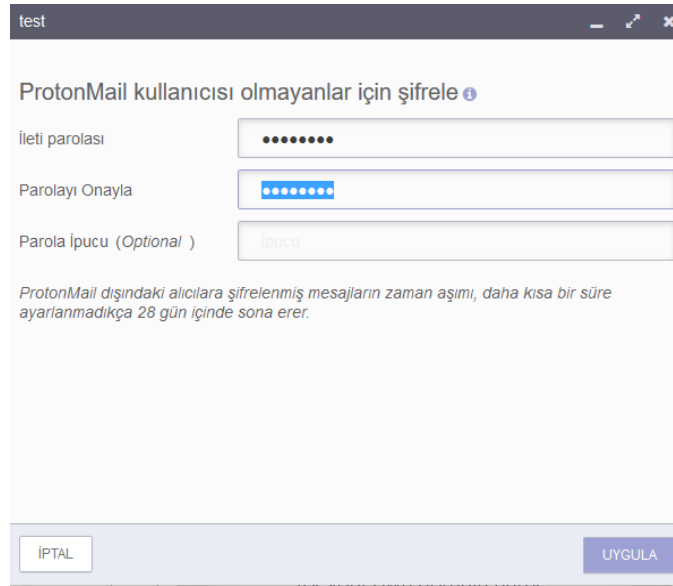


39

Bunu yaptığınızda veya başka bir ProtonMail'a e-posta gönderdiğiniz, mesajın kendi kendini yoketmesi için bir zamanlayıcı ayarlayabilirsiniz. Böylelikle e-posta otomatik olarak hem gönderen hem de alıcı tarafında yok edilecektir. Bu fonksiyonu kullanmanız için aşağıdaki ekran görüntülerine ve yazılara bakınız.

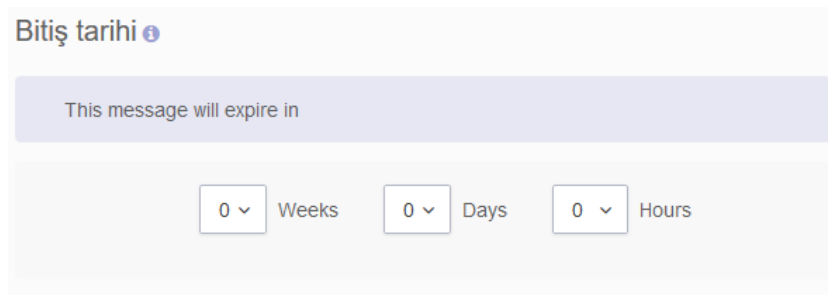
Compose (39) bölümünü açıp yeni bir e-posta hazırlayın. Sol alt köşede üç tuş göreceksiniz; biri ekler için, biri şifreleme/şifre yaratmak için, biri de otomatik yoketme zamanlayıcı için. Şifreleme/şifre yaratmak için olan ortadaki tuşa tıklayın.

Bir şifre yarattın ve Set (40) tuşuna basın. İlk ekrana geri döneceksiniz. Ardından üçüncü tuşa basarak otomatik yoketme zamanlayıcısı bir zaman ayarlayın.



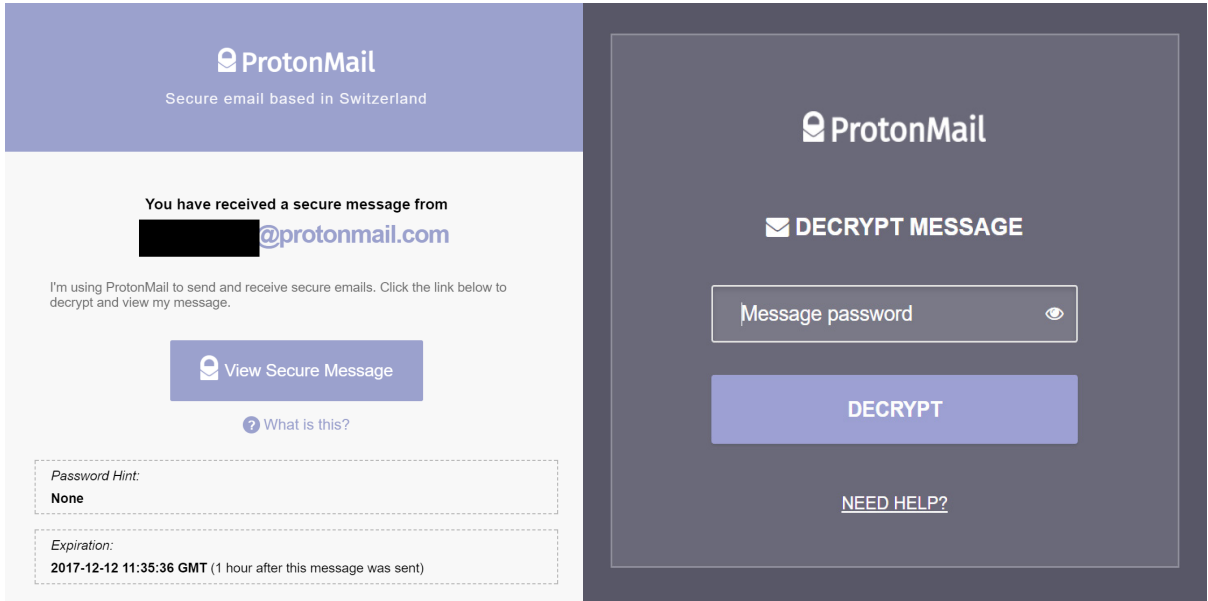
40

Bu zamanlayıcıyı (Son kullanma tarihi) ayarlayın ve tekrar Set'e tıklayıp orijinal pencereye geri dönün (41). Sırasıyla Haftalar, Günler ve Saatler seçebilirsiniz (soldan sağa).



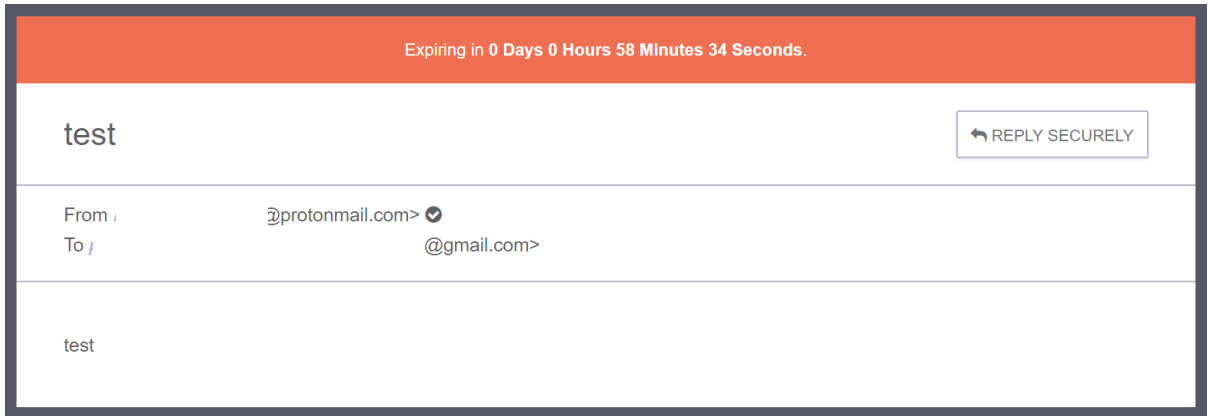
41

E-postayı göndermenizle birlikte alıcı, link içeren bir e-posta alacaktır (42). Bu linke tıkladıklarında şifre girmeleri istenen bir websitesine yönlendirilirler (43). Bu şifreyi girdiklerinde mesajı okuyabilirler (44). Not: Eğer bu mesajı başka bir ProtonMail adresine gönderirseniz, mesaj alıcının gelen kutusunda normal bir mail gibi görünecektir (fakat kendi kendini yoketme zamanlayıcısı aynı şekilde çalışacaktır.). Bu noktada karşınızdaki cevapla tuşuna basarak, aynı şifreyi kullanmak suretiyle size bir cevap gönderebilir.



WIN42

43

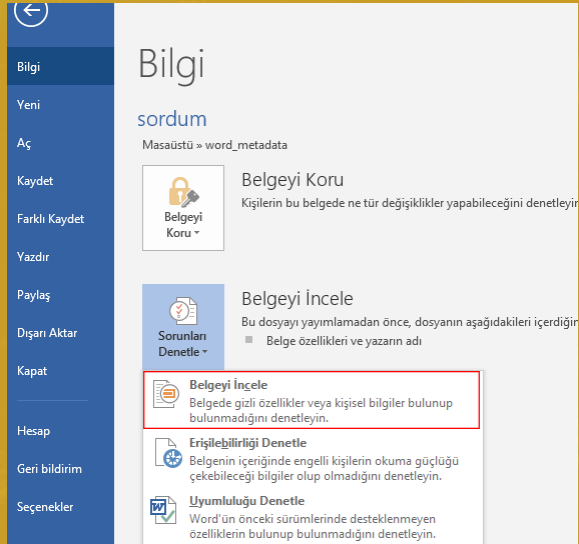


44

EK: METADATA

Metadata, bir şeyin içeriği haricindeki bilgidir. Örneğin bir e-posta için Metadata, e-postanın gönderildiği saat, boyutu, kullandığı IP adresi, mesajın konu başlığı, kim tarafından gönderildiği ve kim tarafından alındığıdır. MS Word belgeleri ve PDF dosyaları için Metadata, dosyanın ne zaman oluşturulduğu (veya düzenlendiği), bunu kimin yaptığı (bilgisayar kullanıcısının adı), yapılan değişikliklerin zamanı gibi bilgilerdir. Bu durum harfiyen MS Publisher, InDesign gibi yayımlama ve tasarım araçları için de geçerlidir.

Günümüzde telefonunuzla çektiğini fotoğraflar ve videolar, bu gibi metadataları içermektedir. Eğer konum erişimi izni verilmişse, açık bir GPS konumuyla fotoğrafın/ videonun nerede çekildiği de bu bilgilere eklenir. Dahası, fotoğraf uygulamaları artık öyle sofistike çalışmaktadır ki çektiğiniz fotoğraflardaki insanları tanıyabilmekte, hatta onları telefonunuzdaki adres defterinizden veya geçmiş fotoğraflarınız üzerinden etiketleyebilmektedirler. Bu bağlamda yayımladığınız bir PDF dosyasının veya



45

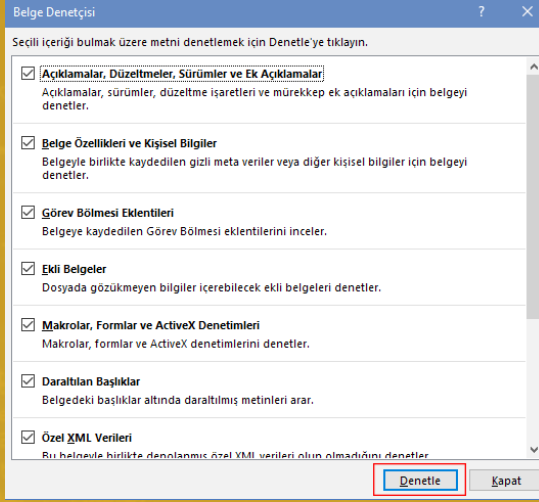
birine gönderdiğiniz bir fotoğrafın ne kadar çok veri içerebileceğini anlamaya çalışın.

Metadata meselesini göz önünde bulundurmanız, düşündüğünüzden daha fazla bilgiyi ortaya saçmadığınızdan emin olmanız için önemlidir. Zira metadata her zaman ardında önemli izler bırakır.

OFFICE BELGELERİ VE PDF'LER İÇİN

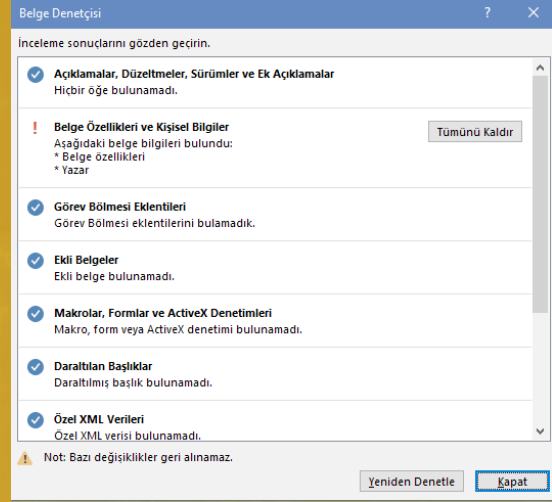
MS Office programları (Word, Publisher, Excel vb.) belgelerden bu gibi metadataları temizleyebilen bazı araçlara sahiptirler. Bu, dosyasınızı kaydetmeden hemen önce metadataları silbilen bir aracı varolduğu anlamına da gelmektedir. Bu araçlar hem Win10'da hem de OSX'de aynı şekilde ve kolaylıkla çalışan işlevlere sahiptirler. Öncelikle Dosya tuşuna tıklayın, bu tuş size aşağıdaki gösterilen sekmeye götürecektir.

(45)'de gösterilen Dosyayı İncele tuşuna tıklayın ve açılır menüden Dosyayı İncele'yi seçin. Beliren pencerede (46) kontrol edilecek maddelerin bir listesini göreceksiniz; burada Dosyayı İncele'ye tıklayın.

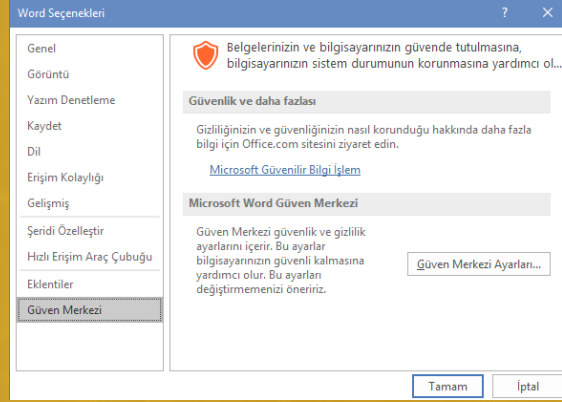


46

İncele tuşuna tıkladıktan sonra açılan pencere, size her madde içerisinde bulunan tüm bilgileri listeyecektir (47). Bu pencerenin sol tarafında Tümünü Sil tuşu bulunmaktadır. Bu tuşa tıklayın ve ardından Kapat'a tıklayın. Belgedeki tüm metadatayı bu şekilde silmiş oldunuz ve artık belgenizi istediğiniz gibi kaydedebilir veya bir PDF'e dönüştürebilirsiniz. MS Word'ün OSX'teki eski sürümleri için biraz daha farklı bir yol kullanmanız gerekmektedir. Belgeyi açın ve sırasıyla Word >



47

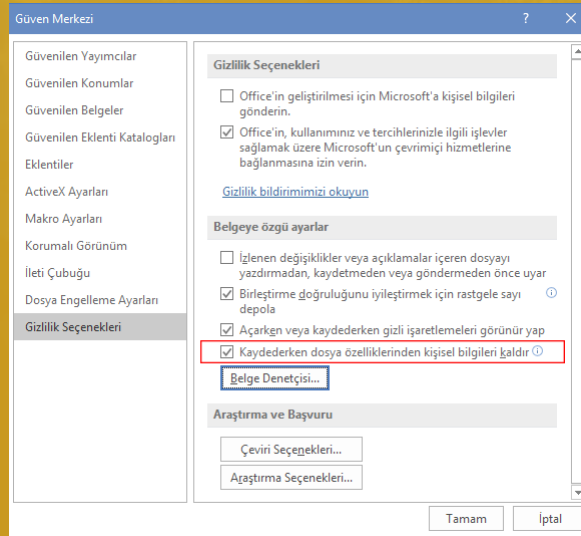


48

Tercihler > Güvenlik başlıklarına tıklayın. Güvenlik bölümünde, Bu Belgedeki Tüm Kişisel Bilgileri Kaydederken Sil'in işaretini kaldırın. (48)

MS OFİS AYARLARI

Şu noktada Office programlarınızın ayarlarına bir göz atmanızda fayda var. Bir Word veya Excel Dosyası açın ve sol üstteki Dosya sekmesine tıklayın. Yan menünün alt kısmında Hesap ve Ayarlar adında iki sekme göreceksiniz. Eğer Hesap sekmesine tıklarsanız (49) bir çok tarayıcı gibi Office programlarının da bir oturum açma işlevinin olduğunu göreceksiniz. Bu işlev Word veya diğer Office programlarını kullanımınızı ve ayarlarınızı senkronize etmeye yarar. Eğer metadata'ları



49

iş dosyalarınızdan ayırmak istiyorsanız, oturum açmayın.

Eğer Seçenekler'e tıklarsanız, yeni bir pencere belirecektir. Burada önemli iki sekme bulunmaktadır. İlki, üstte gördüğünüz Genel sekmesidir. Tam orta kısma bakarsanız (50), burada Kullanıcı İsmi ve Başharfler'e dair girdiler geçreceksiniz. Bunlar belgelerinizde görünecektir, dolayısıyla bu kısımda isminizin doğru yazılmadığından emin olun. Bu kısmı değiştirip kaydedebilirsiniz. Dikkat etmeniz gereken önemli bir diğer sekme de Kaydet sekmesidir. Burada (51)'da görünen iki girdiye dikkat etmelisiniz; Dosya Konumunu Otomatik Kortar ve Varsayılan Yerel Dosya Konumu.

Word veya diğer Office programlarını kullandığınız sürece, çalıştığınız tüm belgeler otomatik olarak arada bir kaydedilmektedir. Bunun amacı bilgisayarınızın beklenmedik bir şekilde kapanması durumunda çalışmanızın tamamını kaybetmenizin önüne geçmektir. Fakat bu kayıtlar, değiştirmedığınız sürece, işletim sisteminizin bulunduğu sabit diskteki Office dosyasına yerleştirilmektedir. Bu kayıtlar ancak dosyanızı kaydedip Word'ü veya diğer bir Office programını kapattığınız zaman silinmektedir.

Bilgileri silme bölümünde öğrendiğiniz üzere bu durum gerçekten bir veriyi silme anlamına gelmemektedir ve büyük bir güvenlik açığı teşkil edebilir. Bu ufak fakat riskli tehditten kurtulmak için Gözet'a tıklayıp, bu kayıtların sizin belirlediğiniz şifreli ve gizli bir sabit diske veya USB'ye kaydedileceği bir dosya seçin.

FOTOĞRAFLAR İÇİN

Bilgisayarınızda olan tüm fotoğraflar için, hem Win10'da hem de OSX'te hali hazırda bulunan, işletim sisteminin kendisinde bulunan özellikleri kullanabilirsiniz. Haricinde internetten bu işi gören başka programları da indirmeniz mümkündür.


Özellikler

Boyut	11,6KB
Sayfa Sayısı	1
Sözcük Sayısı	10
Toplam Düzenleme Süresi	2 Dakika
Başlık	Başlık ekleyin
Etiketler	Etiket ekleyin
Açıklamalar	Açıklama ekleyin
Şablon	Normal.dotm
Durum	Metin ekleyin
Kategoriler	Kategori ekleyin
Konu	Konuyu belirtin
Köprü Tabanı	Metin ekleyin
Şirket	Şirketi belirtin

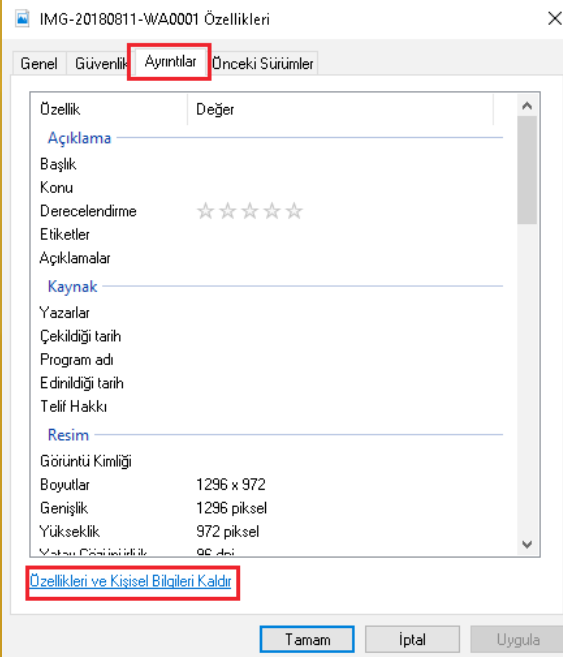
İlgili Tarihler

Son Değişirme Tarihi	Bugün, 11:17
Oluşturma Tarihi	Bugün, 11:16
Son Yazdırma Tarihi	

İlgili Kişiler

Yönetici	Yöneticiyi belirtin
Yazar	 velociraptor

50



IMG-20180811-WA0001 Özellikleri

Genel Güvenlik **Ayrıntılar** Önceki Sürümler

Özellik	Değer
Açıklama	
Başlık	
Konu	
Derecelendirme	☆☆☆☆☆
Etiketler	
Açıklamalar	
Kaynak	
Yazarlar	
Çekildiği tarih	
Program adı	
Edinildiği tarih	
Telif Hakkı	
Resim	
Görüntü Kimliği	
Boyutlar	1296 x 972
Genişlik	1296 piksel
Yükseklik	972 piksel
Yazarın Çizimlediği	96 Adet

Özellikleri ve Kişisel Bilgileri Kaldır

Tamam İptal Uygula

51

Görüntü içeren dosyalarındaki metadata'ları elle silmek istiyorsanız, öncelikle görüntüyü Önizleme'de açın. Menüden Araçlar bölümünü seçin ve Denetleyici'yi seçin. Bilgi panelinde (i) simgesini açın ve GPS'i seçin (52). Bunun ardından Konum Bilgilerini Kaldır'a tıklayın. Bu durum olası tüm konum bilgilerinizi ortadan kaldıracaktır

Özellik Kaldır

Bu özelliklerin bazılarında kişisel bilgileriniz bulunabilir.
[Bir dosyada hangi kişisel bilgiler olabilir?](#)

Dosyada bulunabilecek tüm özelliklerin kaldırıldığı bir kopya oluşturun

Aşağıdaki özellikleri bu dosyadan kaldır:

Özellik	Değer
Açıklama	
<input type="checkbox"/> Başlık	
<input type="checkbox"/> Konu	
<input type="checkbox"/> Derecelendirme	☆☆☆☆
<input type="checkbox"/> Etiketler	
<input type="checkbox"/> Açıklamalar	
Kaynak	
<input type="checkbox"/> Yazarlar	
<input type="checkbox"/> Çekildiği tarih	
<input type="checkbox"/> Program adı	
<input type="checkbox"/> Edinildiği tarih	
<input type="checkbox"/> Telif Hakkı	

Tümünü Seç

Tamam İptal

52

PRATİK DİJİTAL GÜVENLİK

ALT BÖLÜM 7 BİLGİYİ SİLME



Delete

Bu bölüm size bilgilerinizi ve dosyalarınızı nasıl sileceğinizi, hatta silmeye dair bildiğinizi düşündüğünüz çoğu şeyin muhtemelen yanlış olduğunu gösterecektir.

Ne var canım bunda diye düşünebilirsiniz. İstemediğim dosyalarımı Geri Dönüşüm Kutusuna atmayı ben de biliyorum. Burada bilecek ne var?

Böyle düşünüyor olabilirsiniz, fakat bir dosyada sil'e tıkladığınızda veya 'geri dönüşüm kutusunu boşalt' dediğinizde, aslında hiçbir şey silinmemektedir. Aslında dün sildiğiniz, hatta 2 yıl önce kurtulduğunuzu düşündüğünüz bir belge, bilgisayarınızda bunlara ulaşmak isteyen herkesin ulaşımına açık bir şekilde olduğu yerde durmaktadır. Belge Explorer veya Finder pencerenizden kalkmış olabilir, fakat hala bilgisayarınızda var olmaya devam etmektedir. Bu gibi 'silinmiş' dosyalara erişmek bir çok suç çetesinin, size veya iş arkadaşlarınıza zarar vermek isteyen kişilerin en favori yöntemlerinden biridir ve çok temel dosya geri dönüştüren yazılımlar aracılığıyla kolaylıkla gerçekleştirilebilir.

Bir çok insan için silme işlemi kör bir nokta gibidir. Güvenlikli olmayan silme işleminden ötürü karşılaşılabileceğiniz riskleri anlamlık için, öncelikle sabit diskin nasıl çalıştığını anlamamız gerekmektedir. Bu her türlü dijital depolamaya uygulanabilir; USB'ler, SD kartlar, hatta bilgisayarınızın sabit diski. Bu sorunları çözmeyi ve güvenli silme işlemi bir alışkanlık haline getirmeyi burada öğrenmeliyiz.

NOT:

Devam etmeden önce önemli bir bilgiye ihtiyacınız var. Sabit sürücünüz bir HDD mi (Hard Disk Drive) yoksa bir SSD mi (Solid Disk Drive)? Win10 kullanıyorsanız, arama fonksiyonunu açın ve Disk Birleştirici (Disk Defragmenter) donatısını bulun. Programı başlatın. Bu program anında bilgisayarınıza bağlı sabit diskin tipini, bölümlerini, USB'leri vb. gösterecektir.

Bu bölümün çoğu kullandığınız tipik HDD'ye danadır. HDD ne yaygın sabit sürücü tipidir. Fakat elinizde daha yeni, son teknoloji, bir lapto veya yeni alınmış bir harici disk varsa, bunlar SSD olabilir. SSD'ye

sahipseniz, burada yazarların çoğunu uygulamanız mümkün olmayacaktır. SSD'ler için daha aşağıda özel bir bölüm bulunmaktadır, fakat yine de bu bölümü normal şekilde okuyun; zira buradaki bilgileri başka sabit disklere, USB'lere vb. uygulamak isteyebilirsiniz.

DEPOLAMA

Farklı veri depolama formatları farklı çalışır. Bu durum güvenli silme işlemi daha zor yapar. Bu nedenle çalışmak için kullandığınız bilgisayarları, telefonları, hard diskleri ve USB'leri sınırlandırmalısınız.

Tüm dijital depolama (hard diskler, USB'ler vb.) en temel seviyede iki tip veriyi içerir: Boş alan, veya mevcut veriye karşı kullanılan veri. Kullanılan veriniz, yarattığınız ve kaydettiğiniz dosyalarca, videolarca, belgelerce vb. kaplanan alandır. Boş, veya mevcut alansa yeni dosyaları kaydetmek veya indirmek için kullanabileceğiniz kalan bellek miktarınızdır. Fakat boş alan tam olarak "boşaltılmış alan" anlamına gelmeyebilir. Boş alan sadece, bilgisayarınızda hali hazırda kaydedilmiş veriye sahip olmayan bellek paketleri anlamına gelir. Sadece üzerlerine yeniden veri kaydetmek ve yeni bilgiyi depolamak için "boşturlar".

Bir şeyi sildiğinizde veya geri dönüşüm kutunuzu boşalttığınızda, bu veri aslında silinmemektedir. Hala olduğu sabit diskinizde yerde durmaktadır. "Sil" tuşuna basınca olan şey sadece bilgisayarınıza bu veriye artık ihtiyacınız olmadığını anlatmaktır. Bir veri parçası gereksiz olarak işaretlendiğinde, kapladığı alan gelecekte yeni dosyaların kaydedilebilmesi için boş (mevcut) olan olarak kabul edilir. Kullanıcı olarak bu geçmiş veriyi göremezsiniz fakat bahsi geçen veri aslında hiçbir yere gitmemiştir. Bunu üzerlerine yeni dosya kaydedilene dek saklanıyorlarmış gibi düşünün. Fakat Dosya Kurtarma (File Recovery) gibi basit yazılımları bu verileri bulmak kolaydır.

"Silinen" veri hala okunabilir. Dahası, bunu okumak için hiçbir teknolojik yeteneğe ihtiyacınız yoktur. Tek yapmanız gereken ücretsiz bir program indirmektir; ardından bir tek tuşa bastığınız tüm bu dosyalar gösterilir. Bu programlar kanun yürütme tarafından sıkça kullanıldığı gibi, kriminal kişiler/gruplar tarafından da sıkça kullanılmaktadır.

Daha da önemlisi "silinen" verinin kronolojik bir sırayla tutulmadığının farkına varmaktır. Yeni bir veri kaydettiğinizde, bu veriyi eski veya yeni boş alana kaydetmek gibi bir sıra yoktur. Bunun anlamı hangi verinin üzerine yenilerinin kaydedildiğine ve hangi verinin sabit diskinizde kaldığına dair hiçbir beklentiniz olmamasıdır. İşte tam da bu yüzden verilerinizi güvenlice silmek önemlidir.

İşin kötüsü tıpkı bir word dosyası gibi, bir eylemi "geri alabilirsiniz". Belki yanlışlıkla bir paragrafı sildiniz ve ardından onu geri almak istediniz. Bu "geri alma" işlemi burada da gerçekleştirilebilir ve sizin haricinizde biri üzerlerine daha önceden başka dosya kaydedilmiş olsa dahi sildiğiniz bazı dosyalara erişebilir. Kısacası güvenlik için, eski verinin üzerine birden fazla kez "kaydetme" işlemi yapılmalıdır. Ancak bu sayede başkalarının bu verilere erişimi engellenebilir.

Şanslıyız ki bu problemi sizin için çözebilecek programlar mevcuttur. Bu program CCleaner'dır, kullanımı kolaydır ve daha ilerideki Teknik Çözüm: CCleaner bölümünde bulunabilir.

SSD SÜRÜCÜLER

Çoğu sabit diskler HDD'dir (Hard Disc Drives). Zaman içinde bu gibi cihazlardan güvenle veri silmek için çeşitli programlar ve teknikler geliştirilmiştir (örn. CCleaner). Fakat yeni tip bir sabit sürücü olan SSD (Solid State Drive) git gide daha yaygın hale gelmektedir. Bunlar boyut olarak daha küçük fakat daha hızlı ve daha yüksek performanslıdır. Bu nedenle çoğunlukla daha pahalı bilgisayarlar için satılmaktadırlar. Dolayısıyla yeni bir bilgisayara sahip olsanız dahi HDD'ye sahip olmanız muhtemeldir.

İyi tarafı: Laptopunuzdaki SSD sürücüleri otomatikman yeni, özel bir içerikle birlikte gelmektedir. Buna TRIM denir. Bilinen HDD'lere göre çok daha güvenli bir yolla verilerinizi silmenizi sağlayan bir şekilde çalışır. Böylelikle başkalarının 'Dosyalarınızı geri dönüştürmesini' çok daha güçleştirir.

Kötü tarafı: CCleaner (veya benzeri programlar) çalışmaz veya tam anlamıyla fonksiyonel değildirler. Hatta OSX için CCleaner'da bu özellik tamamen kaldırılmıştır. Sahip olsanız dahi çok kullanışlı olmayabilir ve SSD sürücünüzün hızlı eskimesine veya ona zarar vermenize neden olabilir. Normal CCleaner fonksiyonlarının çalışmamasından ötürü, bilginin tamamen ortadan kalkıp kalkmadığı konusunda emin olamazsınız; zira TRIM emrinin ne zaman çalışıp bu bilgiyi sildiğini bilemezsiniz.

TRIM, OSX bilgisayarlarda otomatik olarak etkindir. Win10'daysa çoğunlukla etkindir. Emin olmak istiyorsanız arama bölümüne tıklayın, buraya "Komut İstemi (Comman Prompt)" yazın, buna sağ tıklayın ve "Yönetici olarak çalıştır (Run as administrator)" butonunu seçin. Yeni gelen pencereye şu kodu kopyalayın: "fsutil behavior query DisableDeleteNotify" ve Enter tuşuna basın (buraya "" işaretlerini girmeyin). Gelen cevabın şöyle olması gerekir: "NTFS disabledeletenotify = 0". 0 etkin olduğunu, 1 ise devre dışı olduğunu göstermektedir. "1" gösteriyorsa, şu komutu kopyalayın: "fsutil behavior set disabledeletenotify NTFS 0" ve Enter'a basın. Bilgisayarınız artık TRIM'i etkin kılmaya ayarlıdır.

DOSYALARIN

Bir dosyanın yerini değiştirmenin tam olarak ne anlama geldiğini anlamak önemlidir. Bir dosyanın yerini değiştirdiğinizde basitçe bu dosyanın oynatıldığı yerde bir kopyasını çıkartırsınız. Bu sırada eski konumdaki dosya, üzerine tekrar dosya kaydedilmesini bekler halde tekrar yazılır. Bunun anlamı masaüstünüzde yeni bir word dosyası yaratır (ki bu İşletim Sisteminizin sabit diskinde depolanır) ardından da bunu şifreli bir bölüme alırsanız, eski dosya boş alan olarak işaretlenecek ve başkalarının basit dosya geri dönüştürme programları kullanılarak erişilebilecektir. Aynıısı tarayıcınız aracılığıyla indirdiğiniz dosyaların varsayılan konuma indirilmesi (neredeyse her zaman İşletim Sisteminizin hard diski) ve buradan şifrelenmiş bölümlere alınmasında da geçerlidir.

Başlangıçtan sona kadar dosyaları güvenli bir konumda tutmanın önemli bir nedeni, bu dosyaların arkalarında başkaları tarafından bulunabilecek hiçbir iz bırakmayacakları olmalarıdır. Kısa süreliğine de olsa, örneğin C: sürücünüzde depolanmış herhangi bir dosya, bu sabit sürücüde kullanılacak bir dosya kurtarma programı yoluyla geri edinilebilir. Fakat bir dosyayı doğrudan USB üzerinde depolayıp aynı USB’de tutarsanız, silindiği durumda sadece bu USB üzerinde mevcut olacaktır. Sonrasında CCleaner kullanarak bu dosyaları kolaylıkla ve düzgünce silebilirsiniz.

İşte tam da bu nedente telefonunuzu asla ve katiiyen, her ne sebeple olursa olsun hiçbir çalışma dosyanızı (geçici olarak olsa bile) depolamak için kullanmamanız gerekmektedir. Telefonunuza asla e-postanızdan bir dosya indirmeyin; kısaca okuyup ‘sileceğinizi’ biliyor olsanız dahi!

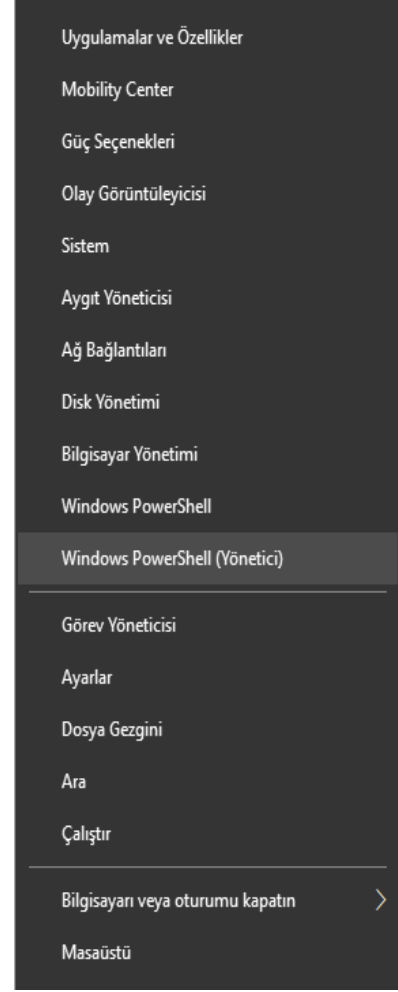
SANAL BELLEK

Son olarak ilaveten, Bölüm 2: Bilgisayarınızı Hazırlamak kısmın Yerel Güvenlik İlkesi (Local Security Network) – Win10’da, kapatıldığı anda “disk belleği dosyasını” otomatik olarak temizleyen bir değişiklik yaptınız. OSX’te bu değişiklik Güvenlik (Security) altında Güvenli Sanal Bellek Kullan (Use Secure Virtual Memory) olarak bulunmaktadır. Bu talimatı size verememizin sebebi böylelikle bilgisayarınızın bellek kullanarak çalışacak olmasıdır, bu da bilginin çalıştığınızın şeyin üzerinde kalmasını sağlamaktır. Kapatma işlemi yaptığınız, RAM ismindeki bu bellek temizlenir. Fakat bilgisayarlar aynı zamanda bunu desteklemek için sabit diskin bir kısmını da kullanır ve bu kısım yaptığınız işlere dair bilgi toplar. Bu “sahte” bellek bir sürü isme sahiptir; sanal bellek (virtual memory), disk belleği dosyası (page file) ve getir götür kütüğü (swap file) bunlardan bir kaçıdır. Hali hazırda yaptığınız bu değişiklik nedeniyle bilgisayarınızı, onu her kapattığınızda bu bilginin düzgünce silineceğini şekle getirmiş oldunuz. Bunu yapmazsanız, sabit diskiniz daha önceden üzerinde çalıştığınız bazı bilgileri içerebilir ve bu bilgiye teknik olarak yetenekli kişilerce erişilebilir. Bu problem burada çözülmüştür.

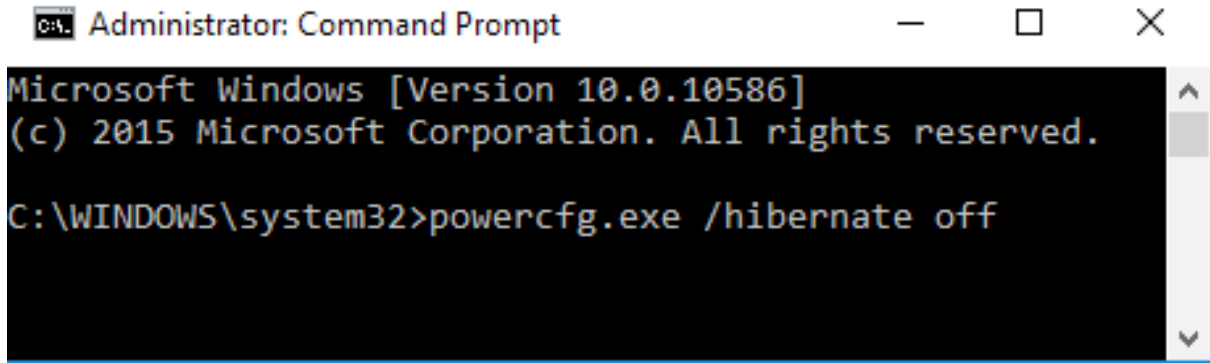
UYKU

Uyku (Hibernation), Win 10’da bilgisayarınızı kapattıktan sonra geri açtığınızdan hızla kaldığınız yerden işinize devam etmenizi sağlayan bir fonksiyondur. Bu fonksiyonu kullanmak çekicidir çünkü işinize çok daha hızlı şekilde devam edebilirsiniz. Bunun altındaki neden İşletim Sisteminizin tüm bilginizi alıp, hard diskinize kaydetmesidir. Sonradan bilgisayarınızı başlattığınızda tüm bu bilgiyi geri yükler. Bunun anlamı eğer bilgisayarınız alındığında ve başlatıldığında, en son üzerinde çalıştığınız her şeyi gösterecektir. Bu bilgi şifreleme olmaksızın depolanır. Bu çok tehlikelidir.

Uyku'yu Win10'da devre dışı bırakmak için arama bölümüne tıklayın ve "Komut Dizini (Command Prompt)" yazın. Kutuya sağ tıklayın, *Yönetici olarak başlat* deyin. Açılan yeni pencereye "powercfg.exe /hibernate off" (burada "" işaretlerini kullanmayın) yazdıktan sonra Enter'a basın 53, 54). Buraya dair genel ayarlar Güç & Uyku bölümü aranarak da bulunabilir.



53



54

- Her zaman çalışma belgelerinizi şifrelenmiş gizli bir bölümde tutun.
- Yeni bir dosya veya belge yaratırken, bunu şifrelenmiş gizli bölümde veya bu belgeyi tutmak istediğiniz depolama bölümünün içinde yapın.
- Dosyaların yerini değiştirirken dikkat edin, arkalarında izler bırakabilirler.
- Telefonunuzla veya pad'inizle iş dosyalarına erişmeyin veya bunları depolamayın.
- Uyku fonksiyonunu kullanmayın. Asıl biçimde Kapat komutunu kullanın

TEKNİK ÇÖZÜM: CCLEANER

CCleaner bir çok sorunu çözmemizi sağlayan küçük bir programdır. Bu programla cihazınızda gerçekleştirdiğiniz bir çok çeşit işlemde arta kalan verileri güvenli bir biçimde silebilirsiniz: Çerezler, geçmiş dosyalar, Microsoft Word’de çalıştığınız belgelere dair bilgiler ve benzeri... Ama programın en önemli yanı bilgisayarınızın boş alanına ve “silinmiş” dosyalarını güvenle tamamen ortadan kaldırmasıdır.

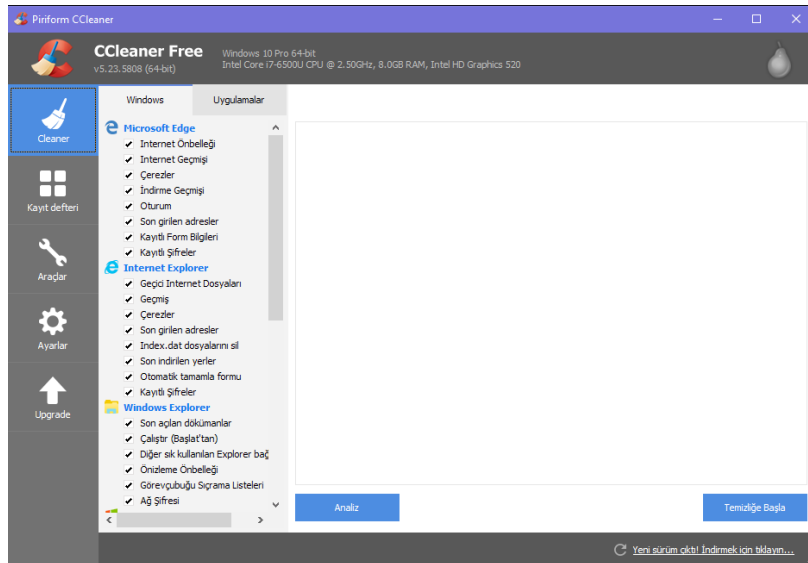
Not: SSD formatında bir sabit diskiniz varsa “Boş Alanı Sil” fonksiyonu kullanışlı, hatta bazı durumlarda mevcut bile olmayacaktır. Fakat diğer tüm fonksiyonlar – geçmiş ve kayıtlarınızı kaldırmak gibi mevcuttur ve bu programı her halükarda yüklemenizi ve kullanmanızı öneriyoruz.

Hem Win10 hem de OSX için programı download.com adresinden indirebilirsiniz. İndirmenin ardından programı yükleyin. Programı masaüstünüzdeki veya uygulamalar klasöründeki simgeye tıklayarak başlatın. Win10’da ayrıca *Geri Dönüşüm Kutusu’na* sağ tıklayıp *CCleaner’ı Aç’ı* seçebilirsiniz.

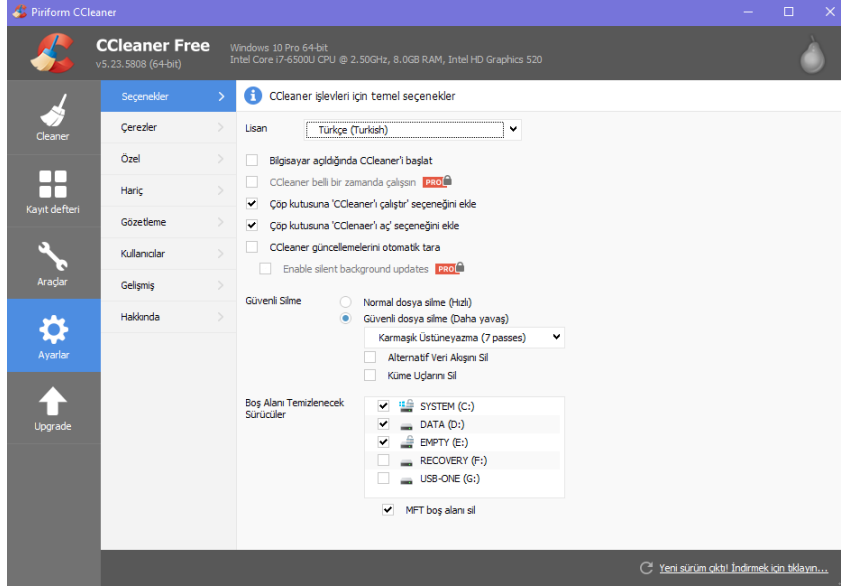
Programı açtığınızda solunuzda bir çok sekme göreceksiniz. Win10 sürümünde bu sekmelerin sayısı fazlayken, OSX’te sadece üç tane bulunmaktadır; yine de bazı ayaları ve seçenekleri bünyesinde barındırmaktadır.

Program Cleaner (Temizleyici) sekmesinde başlar. Sağınızdaki pencerede de iki sekme göreceksiniz; bunlardan biri işletim sistemi için (*Windows veya Mac OSX*) diğeri ise *Uygulamalar* içindir. Windows veya Mac OSX sekmesinin altındaki tüm kutuları seçin. Bunlar, programı çalıştırdığınızda güvenli olarak kaldırılacak farklı tipteki bilgilerdir. Win10’da, listenin en sonunda *Wipe Free Space (Boş Alanı Temizle)* için bir girdi vardır (bunu şimdilik seçmeyin; hele eğer SSD sabit diskiniz varsa **asla** seçmeyin).

Uygulamalar (Applications) sekmesinin altında, neyin güvenli silineceğine dair daha fazla seçenek bulacaksınız. Burada bulacağınız girdiler, bilgisayarınıza neler yüklediğinize bağlıdır. Burada, biri hariç tüm kutuları seçmelisiniz. Eğer kişisel bir tarayıcı kullanmaya karar verdiyseniz ve buradaki bilgilerinizin sürekli silinmesini istemiyorsanız, bu tarayıcının kutusunu işaretlemeyin veya burada silinmesini istediğini kutuları seçin (tarama geçmişinizi silebilirsiniz fakat oturum açma bilgisi gibi şeyleri silmeniz mümkün değildir). 55 kısımdaki örneğe bakınız.

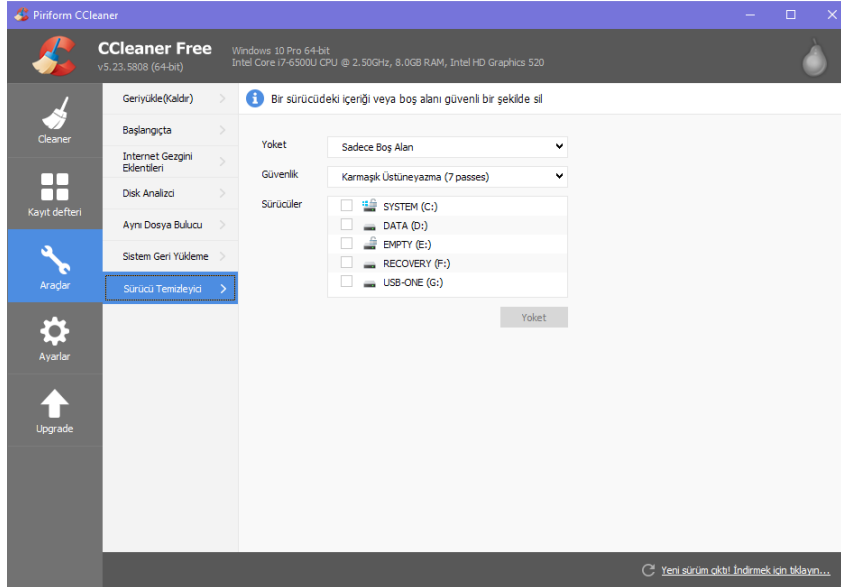


Bundan sonra biraz aşağıdaki *Seçenekler (Options)* tuşuna tıklayın. Karşınıza ilk önce aşağıdaki *Ayarlar (Settings)* alt bölümü çıkacaktır. OSX'te basitçe *Güvenli dosya silme'yi (Secure file deletion)* seçin ve menüden ister *Gelişmiş Üstüne Yazma'yı (Advanced Overwrite – 3 geçiş)* ister *Karmaşık Üstüne Yazma'yı (Complex Overwrite – 7 geçiş)* seçin (56). Geçiş sayısı ne kadar yüksekse, silme işlemi o kadar güvenli yapılmıştır fakat aynı zamanda da bu komutun tamamlanma süresini uzatır.



56

Win10'da 57 takiben aynı seçimi yapabilirsiniz. Ayrıca farklı seçenekleri de gözden geçirebilirsiniz. *Otomatik olarak güncellemeleri kontrol et (Automatically check for updates)* tuşuna tıklayın, aşağıya bakın ve ardından *Boş Alan Temizle* seçeneğini hangi sabit disk(ler) (eğer birden fazla varsa) için uygulamak istediğinizi seçin (55). Bilgisayarınıza o anda bağlı olan USB'ler de burada görünecektir ve bu cihazlarda da *Boş Alanı Temizle* işlemini istediğiniz takdirde gerçekleştirebilirsiniz.



57

Not: CCleaner başladığında şifrelenmiş belleğiniz açıksa/yüklüyse, bu liste de onun da adı çıkacaktır. Bunu eklemenize gerek yoktur. Çoğu zaman sadece ilk sabit diskinizi (C:) seçmek yeterlidir.

Win10'da *Seçenekler* altında *Gelişmiş* adında bir sekme de vardır. Buna tıklayın ve *Uyarı mesajlarını*

sakla'yı (Hide warning messages) seçiniz. Ayrıca Temizlemeden sonra kapat (*Shutdown after cleaning*) seçeneğine tıklayarak bilgisayarınız temizleme işleminin ardından otomatikman kapatılmasını sağlayabilirsiniz.

Son olarak *Araçlar (Tools)* sekmesinin altında *Sürücü Silici (Erase)* adında bir seçenek daha bulunmaktadır (49). Bu size sadece boş alanı - tüm *Temizleyiciyi Başlat (Run Cleaner)* fonksiyonunu kullanmadan, temizleme şansı verir. Boş alanın aslında silmeye çalıştığınız çok eski dosyalar olduğundan bahsettiğimizi hatırlıyor musunuz? Sadece aşağıdaki ekran görüntüsündeki gibi *Sadece Boş Alan'a (Free Space Only)* tıkladığınızdan emin olun, aksi takdirde varolan verileriniz de silecektir.

Şimdi yüklemeyi tamamladınız ve bir test gerçekleştirebilirsiniz. Temizleme sekmesine geri dönün ve *Analiz Et'e (Analyze)* basın. Hızlı bir analizin sonucunda program size nelerin silineceğini gösterecektir. Bu seçili dosyaları silmek için *Temizleyiciyi Çalıştır (Run Cleaner)* tuşuna tıklayın. *Eğer Boş Alanı Temizle (Win10)* ve *Boş Alanı Sil (OSX)* bu işleme ekliyse, komutun tamamlanması daha uzun zaman alacaktır. Sadece İşletim Sistemi'nizden, tarayıcı geçmişinizden vb. kurtulmak istiyorsanız, *Boş Alanı Temizle (Wipe Free Space)* sekmesinin seçili olmadığından emin olun ve ardından geri dönüp *Analiz Et'e* tekrar tıklayın. Herhangi bir word dosyasını, programı veya tarayıcıyı kapatmadıysanız program, silinebilmeleri için size bunları kapatmanızı söyleyecektir.

CCLEANER'I KULLANMAK

CCleaner'ı iki şekilde kullanabilirsiniz; *Boş Alanı Temizle* seçeneğiyle veya bu seçenekten yoksun olarak. *Boş Alanı Temizle*'nin seçili olması, programın çok daha uzun zaman çalışması anlamına gelir (eğer çok küçük bir hard diskiniz yoksa). Eğer basitçe veri izlerinizi silmek istiyorsanız, programı *Boş Alanı Temizle* seçeneğinden yoksun çalıştırabilirsiniz. Bunu sık yapın. Hatta günlük işlerinizi bitirdiğinizde, ideal koşullarda bunu bilgisayarınızı kapatmadan önce gerçekleştirin.

Eğer güvenlik ihtiyacınızın herhangi bir periyotta arttığını hissediyorsanız, bilgisayarınızın sabit disklerinde *Boş Alanı Temizle/Boş Alanı Sil* seçeneklerine zaman ayırmalısınız. Bunu ister *Temizleyiciyi Çalıştır (Run Cleaner)* fonksiyonunu çalıştırırken, sunulan özel *Boş Alanı Temizle (Wiper Free Space)* aracını kullanarak yapabilirsiniz.

WIN10'U KAPATMAK İÇİN CCLEANER'I KULLANMAK

Bu seçenek ne yazık ki OSX için geçerli değildir. Seçenekler bölümünün Gelişmiş sekmesine bakarken, Temizlemenin ardından kapat kutusunu görebilirsiniz. Eğer bunu seçerseniz, Ccleaner işlemleri tamamladıktan sonra bilgisayarınız kapatılacaktır.

Eğer Win10 kullanıyorsanız bunu kullanmanızı şiddetle tavsiye ediyoruz. Bu işlemin ardından bilgisayarınız normal Kapat butonu veya işleviyle değil, CCleaner'la kapatmış olacaksınız. Bilgisayarınız kapanacağı için bu işlemin uzun sürmesinin bir önemi yoktur, zira artık bilgisayarınızın başından ayrılacaksınız.

BÖLÜM III

TELEFON GÜVENLİĞİ

III'ün tamamı telefonları ilgilendiren bir kaç bölümden oluşmaktadır.

8: Telefon Güvenliğini Anlamak size telefonların çalışması hakkında genel bilgiler verecek ve telefonların temel güvenlik meselelerinin neler olduğundan bahsedecektir.

9: Telefonunuzu Kullanmak telefonunuzu daha güvenli şekilde kullanabilmek için neler yapmanız gerektiğine dair rehberlik görevi görecek ve telefonuzla kurduğunuz ilişkiye dair bazı başka meseleleri gündemleştirecektir.

10: Telefonunuzu Ayarlamak, tıpkı bilgisayar kısmındaki Bölüm 2 gibi telefonunuzdaki temel ayarlarla ilgilenen ve bu ayarları güvenliğinizi arttırmak için nasıl değiştirebileceğinize dair fikir veren sıkıcı bir bölümdür. Son olarak

11: Güvenli Uygulamalar ise telefonunuzu güvenli ve etkin şekilde kullanmanızı sağlayacak olan ilgili uygulamaları size sunacaktır.

ALT BÖLÜM 8

TELEFON GÜVENLİĞİ



Bu bölümde akıllı telefonunuzun sizi gözetlemede nasıl kullanılabileceğini, temel tehditlerin neler olduğunu ve telefonunuza yüklü uygulamaların nasıl güvenlik riskinizi arttırabileceğinden bahsedeceğiz.

Günümüzde telefonlar küçük bilgisayarlar gibi çalışıyor olsa da, güçleri sınırlıdır ve bundan ötürü güvenlik tehditlerini çözeniz noktasında da sizi sınırlandırır. Kabaca söylemek gerekirse telefonunuz asla güvenli olamayacaktır. Bu, hatırlanması önemli bir olgudur. Kararsız kaldığınızda veya güvenlik kaygılarınızın arttığı bir durumla karşılaştığınızda, telefonunuzun en zayıf halka olduğunu bilin. Bu gibi ihtimaller karşısında telefonunuzu kapatın, pilini çıkarın ve onu güvenli bir yere bırakın. Pili kendisine takılı olduğu sürece telefonunuz takip edilebilir. Eğer telefonunuzu beraberinizde taşımak zorundaysanız, *Bölüm X: Telefonunuzu Kullanmak* bölümünde "**Karanlığa Karışmak**" kısmına mutlaka göz atın. Veya sadece belirli durumlar için kullandığınız basit bir telefon edinin.

Telefonunuzun size ne gibi problemler yaratabileceğine dair kendinizi test edebilirsiniz. Telefonunuzun SIM kartını çıkarın. Bir yürüyüşe çıkın. Eğer konum özelliğine bakacak olursanız, SIM kartınızın takılı olmamasına rağmen bu özelliğin çalışıyor olduğunu görürsünüz. Eğer Google Maps'te veya başka programlarda hareketlerinizi takip edebiliyorsanız, bu başkalarının da istedikleri takdirde bunu yapabilecekleri anlamına gelir. Bunun nedeni "uçuş modunda" olmadığını sürece, telefonunuzun radyo dalgalarını yakalamaya devam edecek olmasıdır. Telefonlar bu şekilde aramalar, SMS'ler ve jeo-izleme gibi özellikleri için şebekelere bağlanırlar. Bu aynı zamanda SIM karta sahip olmasa dahi telefonların acil aramalara açık olmasının nedenidir. Nihai olarak bu durum üçüncü kişilerin sizi istedikleri anda takip edebilmesi anlamına gelir.

İşte tam burada ilk problemimizle karşılaşıyoruz; **konum izleme**. Konum izleme fonksiyonları çoğunlukla şu şekilde çalışır: Telefonunuz, onu bir arama veya mesaj için kullanmasanız dahi, ara sıra dışarıya bazı radyo sinyalleri gönderir. Bu sinyaller en yakın baz istasyonları tarafından yakalanır. Telefonunuz bu baz istasyonlarıyla sürekli iletişim kurar, böylelikle biri sizi aradığında veya size mesaj attığında bu servisleri size iletir. Büyük şehirlerde çok fazla baz istasyonu bulunmaktadır ve bu baz istasyonlarına telefonunuzun

nerede/ne zaman bağlandığına bakarak üçüncü kişiler telefonunuzun konumunu tespit edebilirler. Bunun isabetliliği bazen bulunduğunuz odayı tespit etmeye kadar gidebilir (üçgenleme, 'triangulation': birden fazla baz istasyonu kullanarak konum tespit etmek). Telefonların ayrıca GPS fonksiyonları vardır ve ayrıca bu fonksiyonların desteklenmesi için telefonlar kablosuz internet bağlantılarını da kullanabilirler. Bunun anlamı telefonunuzun izlenmeye karşı güvenli olduğu an "uçak modunda" olduğu andır (veya çeşitli sinyallere erişiminin engellendiği an). Son olarak telefonunuzdaki bir çok uygulama sizden konumunuzu talep eder ve bu konuda izninizi uygulamanın indirilme sürecinde isteseler de, konumunuza erişim sağladıkları her sefer için sormazlar. Bu durum başkalarına, telefonunuzun konumunu tespit etmek için alternatifler sunmuş olur. Beri yandan konumunuzun izlenmesi, aklınızda bulundurmanız gereken tek problem değildir.

Eğer iş arkadaşlarınız, müvekkilleriniz veya kaynaklarınızla konuşmalarınız dinlenildiğini düşünüyorsanız, telefonunuz bu noktada da bir problem oluşturabilir. Teknik terminolojide akıllı telefonunuzun konuşmalarınızı dinlemek için kullanılan bir cihaza dönüştürülmesine roving bug (hareketli böcek) denmektedir. Fakat basitleştirme amacıyla bu kılavuzda bu terim yerine **gizli dinleme** kavramını kullanacağız.

Konuşmalarınızın gizliden dinlenilmesi için öncelikle sizi dinlemek isteyen kişinin telefonunuzu tespit etmesi gerekir. Eğer SIM kartınız gerçek isminiz üzerine kayıtlıysa bu kolaylıkla gerçekleştirilebilir. Kara borsada bulunan kayıtsız SIM kartlar bu süreci yavaşlatabilseler de, bir güvenlik garantisi oluşturmazlar. Zira sizi aktif olarak izleyen biri telefonunuzun konum sinyallerini takip edebilir, evinizi veya ofisinizi tespit edebilir ve bu yolla kim olduğunuza dair fikir edinebilir. Telefonunuz tespit edildikten sonra telefonunuza erişim sağlanması mümkündür ve bu yolla telefonunuz, mikrofonunun menzili dahilindeki her şeyi kaydeden ve ileten bir cihaza dönüştürülebilir. Bu işlem arkaplanda gerçekleşen bir servistir ve sizin haberiniz olmadan yürütülebilir. Telefonunuzun kamerası da benzer şekilde kullanılarak, kamera menzili dahilindeki her şeyi kaydetmek ve iletmek noktasında sizin haberiniz olmadan çalıştırılabilir. Unutmayın; telefonunuzun mikrofonuna veya kamerasına uzaktan erişim aynı şekilde bilgisayarınız için de gerçekleştirilebilir.

"Telefonunuzun kamerası veya mikrofonu sizin haberiniz olmadan çalıştırılabilir".

Günümüzün akıllı telefonları güvenlik konusunda **daha fazla problem** üretebilmektedir. Geçmişte kullandığımız daha basit cep telefonlarında bu tehditleri ortadan kaldırmak, telefonunuzun pili çıkarmak gibi basit bir işlemle yapılabilirdi. Fakat eski yöntemler artık bu meseleyi çözmeye yetmiyor. Artık bazı telefonlar kapatılsa dahi pillerini yerinden çıkarmak mümkün olmayabiliyor. Veya piller çıkartılabilse dahi çoğu telefon, üretildikleri anda içlerine yerleştirilen küçük bir ilave bataryayla bize ulaşıyor. Bunun nedenlerine; (i) telefonunuzu kapatsanız dahi gece kurduğunuz alarmin sabah çalışabilmesi, veya (ii) telefonunuz kapalıyken başka zaman bölgelerine geçtiğinizde, tekrar açıldığında bulunduğunuz bölgenin saatini görebilecek olmanız, örnek olarak gösterilebilir. Telefonunuzu kapatsanız ve hatta pilini çıkarsanız dahi, yukarıda bahsettiğimiz küçük batarya sayesinde başkaları sizi yine de dinlemeyi başarabilir. Bu nedenle sadece telefonunuzu kapatmak veya pilini çıkarmak tek başına sizi tam anlamıyla koruyamaz.

"...sadece telefonunuzu kapatmak size asla tam anlamıyla koruyamaz".

Elbette başkalarının telefonunuza erişim sağlaması, belgelerinizi okuması, ekran görüntüleri alması (vb.) için **başka yollar** da vardır. Günümüzde bunları gerçekleştirmek için uzman bir hacker olmanıza lüzum yoktur.

Bu gibi tehditlerden ötürü telefonunuza, olabildiğince bir iletişim cihazıymış gibi davranmalısınız; küçük bir iş bilgisayarı gibi değil. Telefonunuza asla hassas dosyalar, belgeler, resimler indirmeyin veya bu gibi verileri telefonunuzda depolamayın. Telefondan herhangi bir veriyi tam anlamıyla silmek çok güç olabilir ve veri silme üzerine olan bölümü hatırlayacak olursanız bir dosyayı silmek, çoğunlukla onu kaldırmak anlamına gelmemektedir. Bu nedenle **geçici süre için bile olsa** telefonunuzu hassas belgeleri depolamak için kullanmayın.

IMSI yakalayıcılar üçüncü kişiler arasında sıkça kullanılan yeni bir araçtır. Telefon gözetimi için küçük, kullanımı kolay ve maliyeti düşüktür. Sıklıkla gösterilerde, büyük toplantılarda veya insanların yoğun olarak bulunduğu benzer etkinliklerde kullanılır. IMSI yakalayıcılar birer baz istasyonumuş gibi davranırlar ve etraflarındaki tüm telefonlar onların bir baz istasyonu olduğunu sanıp buraya bağlanırlar. Bu IMSI yakalayıcılar öylesine küçüktürler ki bırakın onları bir çantaya sokmak, kişisel taşıma ekipmanı olarak bile satın almanız mümkündür. Telefonunuzun şifreleme standardı her zaman baz istasyonu tarafından belirlenir, **telefonunuz tarafından değil**. Bu nedenle IMSI yakalayıcı telefonunuza şifreleme kullanmaması veya çok basit bir şifreleme kullanması emrini verir. Bu yolla başkaları bir bölgedeki tüm telefonları tespit edebilir, sinyallerini veya verilerini kaydedebilir ve bunları okuyabilir. IMSI yakalayıcı kendisi telefonunuzla baz istasyonu arasına yerleştirir. Bu tip saldırılara *aracı saldırılar* (*man in the middle attack*) adı verilir ve bu saldırılar farklı şekilde çalışıyor olsalar dahi bilgisayarlarda ve internet trafiğinde sıklıkla kullanılır.

Son olarak kendinize şunu hatırlatın: Bahsini geçirdiğimiz telefonunuzun fonksiyonları üzerinden karşılaşılabileceğiniz riskler, telefonunuzda bulundurduğunuz uygulamalar üzerinden benzer şekillerde de kolaylıkla karşınıza çıkabilir. Neyi yüklediğinize dikkat edin.

BÖLÜM 8'İN ANAHTAR HATLARI

- Varolan tehdit tiplerinin farkında olun
- Yüklediğiniz uygulamaları sınırlayın
- Telefon ayarlarınızı gözden geçirin ve önceden yükleyip kullanmadığınız tüm uygulamaları silin
- Şüpheli veya tehlikeli bir durumda telefonunuzu kullanmayın, beraberinizde götürmeyin, açık bırakmayın
- Telefonunuzu bir iş bilgisayarı gibi değil, sadece iletişim için kullanın
- Google (hatta daha iyis, DuchGoGo) sizin dostunuzdur – telefonunuzun ayarlarına veya daha önceden yüklediğiniz uygulamalara dair anlamadığınız veya bilmediğiniz her şey için, bunlar aracılığıyla interneti kullanabilirsiniz.

PRATİK DİJİTAL GÜVENLİK

ALT BÖLÜM 9 TELEFONUNUZU KULLANMA



Bu bölüm, telefonunuzu kullanırkenki davranışlarınızın, alışkanlıklarınızın, güvenliğiniz için bir çok teknik çözüme göre nasıl daha büyük bir önem teşkil ettiğini gösterecektir.

TELEFONUNUZ NE

Bir bilgisayarla kıyaslandığında telefonunuzdaki bilgilerinizi etkin bir yolla koruyamazsınız. Şifreleme yapsanız dahi (ki bir çok telefon otomatik olarak şifrelenmiştir) bundan daha gelişkin bir yöntem kullanamazsınız. Telefonunuzun bir kaç güvenlik katmanı vardır ve bu katmanlar PİN kodunuzla telefonunuzu açmaktan tutun, telefonunuzun özel bölümlerine erişebilmeye kadar bir çok şeyi kapsar. Telefonunuzu kaybetmeniz durumunda içerisindeki bilgilerin güvenliği çok ciddi bir sorun teşkil etmez. Fakat telefonunuza zorla el konulduğunda veya başka kişilerce PİN kodunuzu vermeye zorlandığınızda bu durum kritikleşebilir. İkinci durum için çoğunlukla telefonunuz ciddi bir güvenlik zaafı oluşturur.

Korunma sağlarkenki katmanların eksikliği ve tarayıcı kullanmak yerine uygulamalar yoluyla hizmetlere erişmenin yaygınlığı nedeniyle (ayrıca da telefonunuzun tarayıcısının geçmiş izlerini düzgünce temizlemekten ötürü), PİN kodunuzun başkalarının eline geçmesi bu kişilere sadece telefonunuza erişme imkanı değil, aynı zamanda da kullandığınız uygulamalara (dolayısıyla bunlara ilişkin hizmetlere) veya tarayıcınızda kayıtlı bilgilere ulaşma imkanı verir. Bu yolla iyi korunmayan her türlü hizmete üçüncü kişiler kolaylıkla erişim sağlayabilir. Bu nedenle bu kişilerin güvenliğinizi ihlal etmemesi için en temel kurallardan biri, telefonunuzun bir çalışma verilerinizi içeren ikinci bir iş bilgisayarı olmadığını kabul etmenizdir.

“Bir bilgisayarla kıyaslandığında telefonunuzdaki bilgilerinizi etkin bir yolla koruyamazsınız.”

Bunların tamamı telefonunuzun ikinci bir iş bilgisayarı olmadığını anlatmak amacıyla belirtilmektedir. Telefonunuz, asla ve katıyen iş dosyalarınızı sakladığınız, dosyalarınız için bir transfer cihazı olarak kullandığınız bir şey değildir. Ayrıca telefonunuza, bilgisayarınızda kullandığınız çalışmalarınıza ait işlere/ hizmetlere erişim izni vermemelisiniz.

TELEFONUNUZ NE

Yukarıda ve önceki bölümde söylenenlere rağmen telefonunuz, aynı zamanda çok etkin ve güvenli bir haberleşme aracı da olabilir. Burada kilit nokta telefonunuzu sadece ve sadece haberleşme amacıyla kullanmanız ve diğer fonksiyonlarını işin içine çok sokmamanızdır. Bunu başarmak için atmanız gereken sonraki adımsa, haberleşmek için güvenli uygulamaları kullanmanızdır. Otomatik mesaj yoketme özelliğine sahip, kendi kayıtlarını silebilen mesajlaşma uygulamaları, telefonunuza başkalarının erişim sağladığı durumda bu kişilerin yazışmalarınızı görememesini sağlar. Uçtan uça şifrelenen ve kendi kendini otomatik olarak yokeden mesajlar (veya mesaj geçmişleri), haberleşme için çok güçlü ve verimli bir araçtır.

KARANLIĞA KARIŞMAK

Telefonunuzun her tür iletişim ağıyla bağlantısının kesilmesi anlamında kullanılan 'karanlığa karışmak' (Going dark) kavramı, telefonunuzun size karşı kullanılmayacağını tek yoludur. Eğer bir görüşmedeyken ve konuşmalarınızın dinlenilmediğinden emin olmak istiyorsanız, elinizdeki tek çözüm budur. Benzer şekilde kameranızın size kaydetmesini istemiyor veya kesin konumunuzun öğrenilmesini istemiyorsanız, karanlığa karışmalısınız. Bunu bir kaç yolla yapabilirsiniz; en kolayı Uçuş Modu'nu kullanmaktır. Bu yolla hücresel şebeke iletimini (telefonunuzun baz istasyonlarıyla iletişimini), kablosuz internet bağı ve Bluetooth özelliğini durdurabilirsiniz. GPS sinyallerini almaya devam edip etmeyeceği, telefonunuzun tipine göre değişir. Fakat akıllı telefonlar sadece GPS verisini sadece alır, bu verileri iletemezler. Bu diğer iletim biçimlerinin kesilmesi durumunda güvende olacağınız anlamına gelir.

Burada oluşabilecek bir güvenlik zaafiyeti, telefonunuzdaki bir uygulamanın sizin bilginiz dışında veri iletimi gerçekleştirme olabilir. Eğer telefonunuz bir hedef haline gelmişse, bunun gerçekleştirilme ihtimali vardır. Buna benzer bir başka zaafiyetse GPS'inizi açık bıraktıysanız konum verilerinizin kaydedilecek olması ve Uçuş Modu'ndan çıktığınızda kullandığınız bir uygulama aracılığıyla (yine bilginizin dışında) bu verilerin başkalarına iletilebilecek olmasıdır.

Karanlığa karışmanın bir başka kolay yolu da bir alüminyum folyo kullanmaktır. Hassas meseleler üzerine çalışan ve risk altında olduğunu düşünen bir çok kişi, çantalarının içinde bir kaç kat alüminyum folyoyla gezerler. Telefonunuzu iki kat folyoyla kaplayarak (telefonunuzun her tarafını kapatmış olmanız gerekir) benzer şekilde telefonunuzun dış dünyayla iletişimi kesebilirsiniz. Karanlığa karışmak için en iyi yöntem budur. Günümüzde online alışveriş siteleri, içleri folyoyla kaplı özel telefon kapları satmaktadır. Bu kaplar da aynı görevi görmektedir. Deneyip test etmenizi öneririz. Telefonunuzu iki kat folyoya sarın ve aramaya çalışın. Telefonunuza bir mesaj veya e-posta gönderin, bu mesajların telefonunuza erişip erişmediğine bakın. Eğer telefonunuzun bunları alabiliyorsa, bir kat folyoyla daha sarmanız gerekebilir. Yine de bu yöntemi kullanacaksanız, her ihtimale karşı işleyip işlemediğini mutlaka test ettikten sonra kullanın.

“Telefonunuzu iki kat folyoyla kaplayarak (telefonunuzun her tarafını kapatmış olmanız gerekir) benzer şekilde telefonunuzun dış dünyayla iletişimi kesebilirsiniz”

VE YEDEKLEME

Telefonlar için bir başka önemli güvenlik tehdidi de, günümüzde telefonların otomatik olarak bir çok hizmete bağlı (oturumu açık) şekilde gelmesidir. Bu uygulamaların bir tarayıcıya nazaran çoğunlukla çok daha dar

bir bir hizmet arayüzü bulunmaktadır. Fakat bu uygulamalara erişim çoğunlukla şifre veya PIN koduyla korunmaz. Bu nedenle telefonunuza erişim, telefonunuzda kurulu bu hizmetlerin hepsine erişim anlamına gelir. Bu tehlikenin büyüklüğünü azımsamayın. Bilgisayarınızın tarayıcısıyla eriştiğiniz, çalışmalarınızda kullandığınız hizmetlerin uygulamalarını asla telefonunuza yüklemeyin; biliyoruz, bu çoğunlukla işlerinizi kolaylaştırmaktadır fakat aynı zamanda da büyük bir güvenlik açığı oluşturmaktadır. Benzer şekilde hem telefonunuzda hem de bilgisayarınızda aynı bulut depolama hizmetlerini (veya benzer online hizmetleri) kullanmayın. Cihazlarınızda ayrı ayrı oturumlar ve hizmetler kullanın. Eğer bulut depolama kullanmakta ısrarcıysanız, telefonunuzda ve bilgisayarınızda ayrı ayrı hizmetler kullanın (örneğin bilgisayarda Google Drive, telefonda DropBox). Çalışma bilgisayarınızla telefonunuzun kullandığı hizmetleri birbirinden ayırın.

Güvenliğiniz için kavramanız gereken şey, telefonunuzun kullanımını çeşitli alanlarda sınırlandırmak ve telefonunuzu bir haberleşme cihazı olarak görmeye çalışmaktır. İşinizle alakalı meselelerde kullanılacak bir cihaz değil! Telefonunuzdan işinizle ilgili online araştırmalar yapmayın, belgeler indirmeyin veya işinizle alakalı dosyaları burada depolamayın.

Uçuş modu, NFC'yi de (Android'de bazen Beam adıyla da geçer) açabilir. Bu kısa mesafeli bir iletim sistemidir. Kabaca tarif etmek gerekirse iki telefonu yan yana koyduğunuzda, bu telefonların birbiriyle haberleşmesini ve veri transferi gerçekleştirmesini mümkün kılan bir özelliktir.

TELEFONUNUZU KILMAK ÜÇ TEMEL ADIM

Önümüzdeki iki bölüme geçmeden önce aşağıda açıklayacağımız üç temel adımı atmanız gerekmektedir.

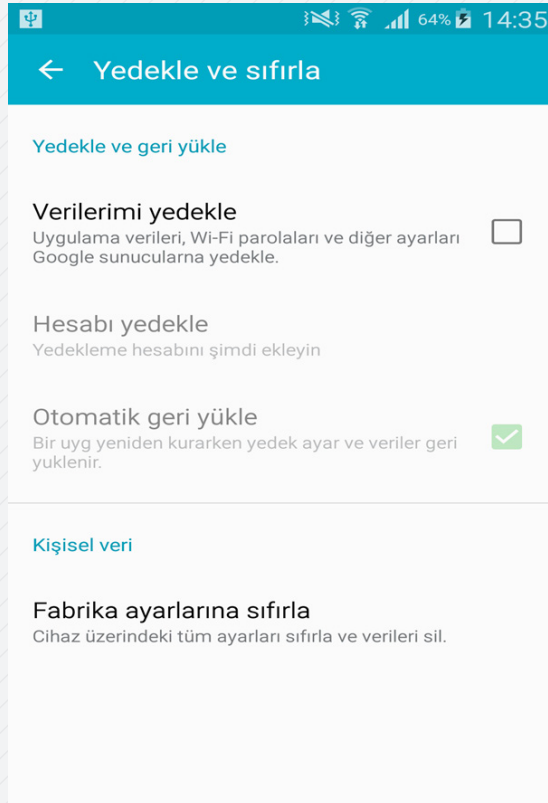
“Çalışma bilgisayarınızla telefonunuzun kullandığı hizmetleri birbirinden ayırın.”

FABRİKA AYARLARINA SIFIRLAMA (FACTORY RESET)

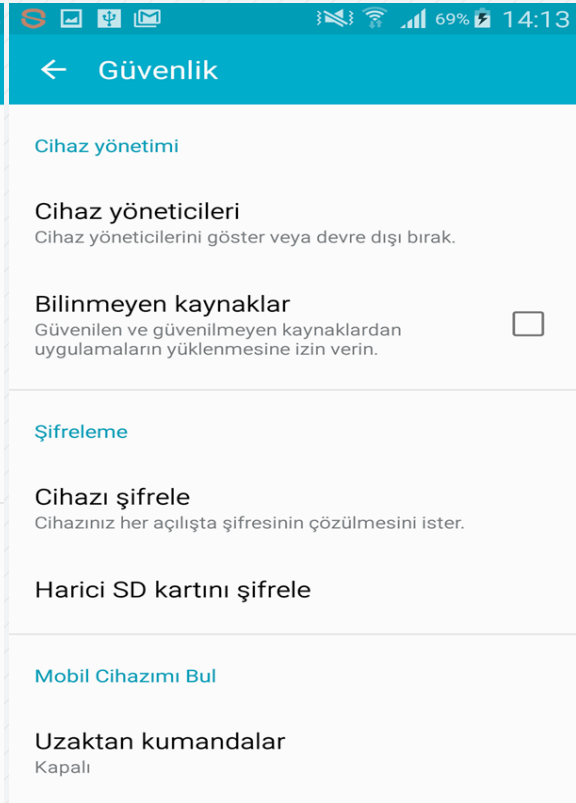
Eğer telefonunuzda bulunan her şeyi tamamen kavradığınızı düşünmüyorsanız, onu güvenli hale getirmeye telefonunuzu fabrika ayarlarına sıfırlayarak başlamalısınız. Bu işlem telefonunuzda bulunan her şeyi kaybedeceğinize anlamına gelir; bu nedenle tutmak istediğiniz dosyaları, fotoğraflar veya diğer dosyaları yedekleyin.

ŞİFRELEME

Telefonunuz kendiliğinden şifrelemesi etkin halde gelir. Fakat Android’iniz varsa bu durumu kontrol etmekte fayda vardır. Telefonunuz ve içerisindeki SD kartı kolaylıkla şifrelenebilir. Fabrika ayarlarına dönüşü gerçekleştirdikten sonra ilk yapmanız gereken (açık olmadığı takdirde) şifrelemeyi etkin hale getirmek ve uygun bir PİN kodu veya şifre seçmektir. Bu işlemi gerçekleştirirken SD kartları da (eğer varsa) içerecek şekilde yapın. (58)



58



59

iOS telefonlar için bu otomatiktir. Ayarlar kısmının Dokunmatik Kimlik & Şifre bölümünde bir PİN veya Şifre seçtiğiniz anda, cihazın tamamının şifrenmesi otomatik olarak etkinleşecektir. (59) Android telefonlar için, Ayarlar kısmında Güvenlik bölümüne gitmeniz ve Cihazı şifreleme tıklamanız gerekir. Cihaz sizden bir PİN kodu veya şifre istedikten sonra süreci başlatacaktır. Hiçbir veri silinmeyecektir. Ayrıca harici SD kartınızı da şifreleyebilirsiniz ve telefonunuz bir SD kart kullanıyorsa, bu işlemi cihazını şifreledikten sonra gerçekleştirmelisiniz.

KALDIR/SİL

Fabrika ayarlarına sıfırlamayı ve şifrelemeyi tamamladıktan sonra, telefonunuzda yüklü Uygulamalar ve Hizmetler'e bir göz atın; kullanmayacaklarınızı silin veya devre dışı bırakın. Bir çok telefon fabrika ayarlarına geri döndürülse dahi bir çok uygulamayla yüklü olarak gelir. Hepsinden kurtulun; bu güvenliğinizi arttıracaktır ve aynı zamanda telefonunuzu hızlandıracak, pilinin daha uzun süre dayanmasını sağlayacaktır.

PRATİK DİJİTAL GÜVENLİK

ALT BÖLÜM 10 TELEFONUNUZU HAZIRLAMA



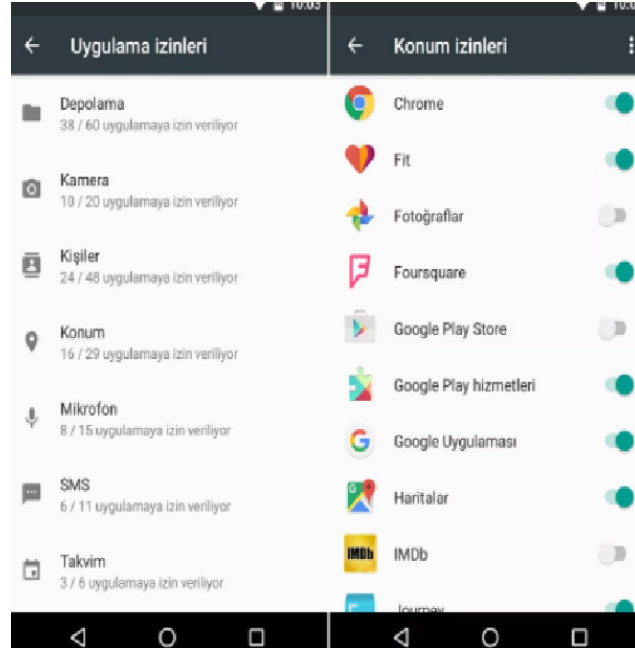
Artık telefonunuz ayarlar bölümüne girip, temel güvenliğinizi için bazı değişiklikleri yapmaya hazırız. Android telefonların bir çoğunun farklı görünümlere, arayüzlere, menü ve ayarlar bölümlerine sahip olmalarından (fakat çoğunlukla da aynı isimlere sahip olmalarından) ötürü, size bu kavramların isimlerini vereceğiz ve telefonunuzun ayarlar bölümünde ilgili başlıkları sizin bulmanızı isteyeceğiz. Daha önceden adım adım ekran görüntüleriyle yaptığımız işlemler, menülerin farklılık göstermesinden ötürü burada manasız bir kalabalık yaratabilir. Ayrıca bu yolla telefonunuzun ayarlarına daha hızlı ısınabilir, telefonunuzu daha kişisel bir hale getirebilirsiniz.

Telefonların işletim sistemlerindeki farklardan, farklı Android üreticilerin farklı seçenekler kullanmasından ve farklı telefonların farklı terminolojilere sahip olmasından ötürü bu ayarların isimlerinde ufak farklılıklar olabilir. Eğer aşağıdaki talimatlar telefonunuzda iş görmezse, gerekli değişiklikleri yapmak için Google veya DuckGoGo'yu kullanabilirsiniz.

AYARLAR VE UYGULAMA

Hem iOS hem de Android telefonlar için, öncelikle Ayarlar bölümünün üzerinden geçeceğiz. Android'de özel olarak Google Ayarları bölümüne sahipseniz, burayı da gözden geçireceğiz.

Telefonunuzu kontrol etmenin ve uygulamaların işlevlerini sınırlandırmanın en kolay yolu, Uygulama Yöneticisi'ne gidip her uygulamaya ayrı ayrı tıklayarak bu uygulamaların her birinin hangi alanlarda hakları olduğunu seçmektir; örneğin takviminize, kameranıza, konumunuza erişim gibi. Bazı telefonlardaysa, telefona dair Konum, Mikrofon vb. her hizmet için, bu hizmetlere hangi uygulamaların erişimi olduğunu listeleyen bir sistem vardır (52).



60

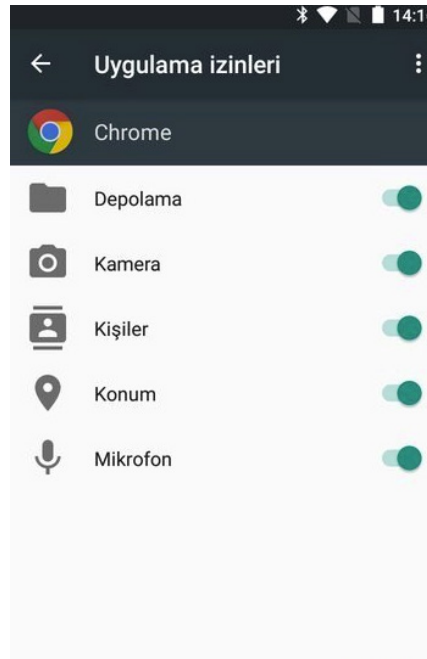
SAMSUNG: Ayarlar > Uygulamalar > Uygulama Yöneticisi

VEYA

SAMSUNG: Ayarlar > Gizlilik ve Güvenlik > Uygulama İzinleri

ANDROID:

Ne yazık ki çoğunlukla uygulamalar, ihtiyaçları olmasa dahi (hatta bu izinleri kullanamayacak olsalar dahi) telefonunuza dair maksimum erişimi talep edeceklerdir. Bu nedenle biraz zaman ayırıp yukarıda belirttiğimiz bölümlerin üzerinden geçmeniz ve tüm izinleri kontrol etmeniz önemlidir. Bu, uygulamaların telefonunuzda neleri kullanabileceğini kontrol altında tutmanın en iyi yoludur (61).



61

Bu ayrıca iki seçeneğiniz olduğunu anlamına gelir. İsterseniz telefonunuzdaki bir hizmeti tamamen kapatabilirsiniz/erişime açabilirsiniz (örneğin, Konum hizmetini), isterseniz de uygulamaları bir mikro yönetime tabi tutup izinlerini ayarlayabilirsiniz. Aslen bir hizmeti tamamen kapatmanız bu konudaki en iyi yöntemdir fakat bu durum her zaman durumunuza uygun veya sizin için etkin olmayabilir. Eğer bir hizmeti açık bırakırsanız, yukarıda bahsettiğimiz işlemleri mutlaka uygulayın ve ara ara, özellikle yeni uygulamalar yüklediğinizde, bu işlemi tekrarlayın.

Konum, Kamera ve Mikrofon dikkat etmeniz gereken üç önemli hizmettir. Bunların dışında kalan izinleri, örneğin SMS'lerinizin okunması/gönderilmesi, belleğinize erişim, takvim, kişiler listesi, e-postalarınızın okunması/gönderilmesi vb. çok daha kolay bir biçimde kontrol edebilirsiniz.

Kullanmadığınız bağlantı tiplerini de kapatmanızı öneriyoruz. Wi-Fi haricinde bağlantılar olarak telefonunuz Bluetooth, NFC ve bazı durumlarda Android Beam hizmetini sunabilir. Aktif olarak kullanmadığınız sürece bu bağlantıları kapalı tutun. Bunlar kısa mesafeli kablosuz bağlantı seçenekleridir ve sık sık kullanmadığınız sürece bunları açık tutmanın bir anlamı yoktur.

(SAMSUNG: Ayarlar > Bluetooth + NFC ve Ödeme+ Daha fazla bağlantı ayarları > Çevredeki cihazları aramayı kapat)

(Android: Ayarlar > Bluetooth + Kablosuz & Bağlantılar > Daha fazlası...)

Neler yüklenebilir? Güvenlik ve gizlilik bölümünde, Bilinmeyen Kaynaklar'a izin vermeye veya bu izni kaldırmaya dair ayarlar göreceksiniz. Bu izni mutlaka kaldırmalısınız. Bu yolla resmi telefon mağazası (örneğin Google Play) tarafından onaylı olmayan herhangi bir programın veya uygulamanın telefonunuza yüklenmesinin önüne geçecektir. Özel bir program yüklemek istediğinizde bu özelliği basitçe kapatabilir, programı yükleyebilir ve ardından özelliği geri açabilirsiniz. iOS telefonlar için bu konuyla uğraşmanıza gerek yoktur zira standart olarak bu telefonlara sadece Apple Store Uygulamaları yüklenebilir.

(ANDROID: Ayarlar > Güvenlik)

(SAMSUNG: Ayarlar > Ekran kilidi ve güvenlik)

EKRAN KILIDI, VE YOKETME

Eğer başkalarının telefonunuzdaki mesajlara veya benzeri haberleşme kaynaklarına erişimini engellemek istiyorsanız, kilit ekranınızı korumak önemlidir. Çoğu telefon önceden ayarlı biçimde, bildirimlerinizi kilit ekranınızda tamamen gösterecek şekilde gelirler. Yani, kilit ekranınızın kodunu girmeden bile bu bildirimler üzerinden bir başkası yeni mesajlarınızı, e-postalarınızı vb. okuyabilir. Bunu değiştirmeniz gerekmektedir. Yukarıda bahsettiğimize benzer şekilde isterseniz bildirimlerinizi tamamen saklayabilirsiniz, isterseniz de teker teker hangi uygulamaların kilit ekranında bildirim gösterebileceğine listeden siz karar verebilirsiniz. Seçiminiz ne olursa olsun, işiniz için kullandığınız hiçbir uygulamanın kilit ekranında bildirim göstermemesini sağlamalısınız.

(SAMSUNG: Ayarlar > Kilit ekranı ve güvenlik > Kilit ekranındaki Bildirimler)

(ANDROID: Ayarlar > Güvenlik)

(ANDROID: Ayarlar > Ses & Bildirimler > Cihaz Kilitliken ('Hassas bildirim içeriğini sakla'yı seçin)

Ayrıca telefonunuzda hangi uygulamaların bildirim gösterebileceğine de karar verebilirsiniz (kilit ekranındakiler değil). Bazı uygulamalardan hiçbir şekilde bildirim almak istemeyebilir, bunları sadece elle kendiniz açıp görmek isteyebilirsiniz.

(SAMSUNG: Ayarlar > Bildirimler)

(ANDROID: Ayarlar> Ses ve Bildirim)

(ANDROID: Ayarlar > Ses & Bildirim > Uygulama bildirimi)

(ANDROID: Uygulamalar > İzinler VEYA Uygulamalar > Dışlı simgesine tıklayın > Uygulama İzinleri'ni seçin)

Kilit ekranıyla uğraşırken, Otomatik Kilit özelliğini etkin kıldığınızdan ve bunun süresinin 5-10 saniye gibi kısa bir süre olduğundan emin olun. Eğer imkanınız varsa, güç tuşuyla kilitlemeyi de aktifleştirin (telefonun güç düğmesine bastığınızda ekranın kilitletmesini sağlar). Son olarak Otomatik Fabrika ayarlarına dönüşü etkinleştirin. Bu son ayarın özelliği, PIN kodunuzun 10 veya 15 kez yanlış girilmesi durumunda telefonunuzun kendi kendini otomatik olarak fabrika ayarlarına döndürmesidir (reset).

(SAMSUNG: Ayarlar > Kilit ekranı ve güvenlik > Güvenli Kilit ayarları)

(ANDROID: Ayarlar> Güvenlik)

Şifrelemeyi açtığınız anda zaten bir PIN kodu veya şifre seçmişsiniz. Fakat herhangi bir nedenden ötürü bu durum Kilit Ekranınız için geçerli değilse mutlaka bunun etkinleştirildiğinden emin olun. Ayrıca eğer telefonunuz parmak iziyle (dokunarak), sesle, yüz veya retina (göz) tanımayla açılma özelliğine sahipse, bu özelliği kapatın.

GÜNCELLEMELER

Bilgisayarınız gibi telefonunuz da en yakın tarihli güncellemesi kadar güvenlidir. Telefonunuzda otomatik güncellemelerin açık olduğundan emin olun.

(SAMSUNG: Ayarlar > Cihaz Hakkında)

(Android: Ayarlar > Telefon Hakkında)

VE BULUT DEPOLAMA

Telefonunuzda varolan tüm bulut hizmetlerini tespit edin. Bunlar ayarlar bölümünde görünecektir. Üzerilerinde gerekli değişiklikleri yapın. Bu tip bulut hizmetlerinin kapalı olduğundan veya işinizle alakalı verileri içermediğinden emin olun. Eğer Bulut temelli yedekleme veya depolama kullanmak istiyorsanız, lütfen Bölüm 6: Bilgiyi Paylaşmak bölümünü tekrar ziyaret edip, bu hizmetleri en iyi şekilde nasıl kullanacağınızı iyice öğrenin.

TELEFON AYARLARINA SON KAÇ NOT

Android ve iOS bazlı telefonlarınız için reklamları kapatın; Anroid için 'İnternet bazlı reklamlar' kısmını devre dışı bırakın ve iOS için 'Reklam Takibini Sınırla'yı etkinleştirin.

(iOS Gizlilik > Reklam)

(Android Google Ayarları > Reklamlar)

Güvenlik için, sesli komut fonksiyonlarını (OK Google, Cortana, Siri, vb.) ya kapatmalısınız ya da bunların Kilit Ekranı devredeyken çalışmadığından emin olmalısınız.

GÖZ ÖNÜNDE BULUNDURMANIZ GEREKEN KAÇ UNSUR:

- Yeni mesajların, e-postaların vb. kilit ekranından doğrudan okunamayacağından emin olun.
- Hangi uygulamaların/fonksiyonların ne zaman konumunuzu kullanabileceği konusunda mutlak kontrol ve bilgi sahibi olun.
- Farklı uygulamaların hangi izinlere tabi olduğunu kontrol edin, gerekli değişiklikleri yapın.
- Kameranızın konumunuza erişimi olmadığından emin olun.

EK: KONUM İZLEME

Eğer izlenme ihtimallerinden gerçekten kaçınmak istiyorsanız, telefonunuzun sadece 'karanlığa karışmasının' bu problemi tamamen çözemeyeceğinin bilincinde olun. Arabanız otomatik olarak yol güvenliği kameraları tarafından, otoyol gişelerince ve şehir içinde MOBESE'lerce tespit edilebilir, konumu belirlenebilir. Aynı şekilde kredi/banka kartlarınızı, veya adınıza kayıtlı herhangi bir kartı (örneğin toplu taşıma araçları için kullandığınız pasonuz, kütüphane kartınız vb.) kullandığınız anda konunuz tespit edilebilir. Fotoğraflarınızı internette paylaşan arkadaşlarınız, farkında olmadan konumunuzu ve bu konumda bulunduğunuz zamanı da paylaşmış olurlar ve başkaları sizi izlemeye karar verdiyse bu fotoğraflarla sizi bulabilirler.

Uzun periyotlar (hatta bazen kısa periyotlar) için karanlığa karışmak neredeyse imkansızdır; özellikle de bu süreç için gerekli nakit, ulaşım vs. hazırlıklarını yapmadıysanız. Günümüzde bir alışveriş merkezindeki normal güvenlik kameraları dahi yüzünüzdeki karakteristik özelliklerden size tanıyabilir, hatta bunu çok hızlı yapabilirler. Bu teknolojilerin ne kadar sofistike hale geldiklerini azımsamayın.

Telefonunuz, kendisine ait özel kimlik numaralarıyla da tespit edilebilir. Bunlardan biri donanımına özgü bir numaradır, diğeriye SİM kartınıza işlenmiştir. Bu numaralara IMEI (telefonunuz için) ve IMSI (SİM kartınız için) numaraları denir. Bu numaralar baz istasyonlarına ve veri/telefon hizmeti sağlayıcılara kayıtlıdır. Bu eşsiz numaraları saklayamaz veya değiştiremezsiniz. Eğer telefonunuz biliniyorsa, IMSI numaranızın da biliniyor olması muhtemeldir. Telefonunuza el konulduysa/kaybettiyseniz, IMEI numaranıza erişilebilir ve telefon hizmeti sağlayıcınıza danışılarak bu numara aracılığıyla verilerinize ulaşılabilir. Bu yolla üçüncü kişiler tüm meta verilerinizle (geçmişe dönük çok uzun periyotlar için konum, aradığınız numaralar, kullandığınız veriler vb.) hareketlerinizi haritalandırabilir. Unutmayın; telefonunuz ciddi bir risktir ve bir iş aracı olarak kullanımı sınırlandırılmalıdır.

Kısaca kendinizi bu durumlara düşürebilecek adımları asla atmayın. İşiniz çok çok önemlidir; fakat güvenliğiniz bundan önce gelmektedir. Güvenliğiniz, işinizde pes etmemenizin en önemli ayağıdır.

PRATİK DİJİTAL GÜVENLİK

ALT BÖLÜM 11

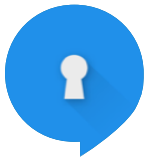
KUYLLANILABİLİR GÜVENLİ UYGULAMALAR



Bu bölümde size yapılmasını istediğiniz işleriniz daha güvenli ve verimli şekilde yapabildiğiniz bir dizi uygulama ve program sunacağız: Telefonunuzun sahip olduğu SMS programını, aynı işi uçtan uça şifreleme de yapabildiğiniz başka tip programla değiştireceğiz, TOR'un internetteki hareketlerinizi nasıl sınırsız ve daha güvenli hale getirdiğinden bahsedeceğiz ve sadece şifreleme yapmakla kalmayıp, aynı zamanda otomatik olarak yazışma geçmişlerinizi yokeden mesajlaşma (chat) programlarını anlatacağız.

Bir uygulamayı yüklediğinizde, mutlaka ayarlar bölümüne gidip uygulamanın kendi ayarları hakkında bilgi edinin. Signal ve Telegram gibi bazı güvenli uygulamalar, yükledikleri anda kendileriyle birlikte gelen PİN kodlu veya şifreli koruma katmanlarına sahiptirler. Bunun anlamı bu uygulamanın, kendisi için bireysel bir PİN kodunun ayarlanmasına müsaade etmesidir. Telegram ve Signal için, bu mutlaka yapılması gereken bir şeydir. Fakat diğer yandan bir çok uygulamada bu özellik yoktur. Her uygulama için özel bir PİN kullanarak, akıllı telefonunuza erişim gerçekleştirilse bile, bazı spesifik uygulamalar bloklanacak ve bu nedenle güvende kalacaklardır

SMS VE TELEFONLA ARAMALAR



Signal Private Messenger yükleyin; hem telefonla arama hem de mesajlaşma için bu programı kullanabilirsiniz. Signal kullanarak SMS gönderdiğinizde (Ayarlar > SMS ve MMS > SMS Etkin'i seçin) veya bir arama yaptığınızda işlemlerinizi, otomatik olarak uçtan uça şifrelenecek ve böylelikle de SMS ve telefon konuşmalarınız dinlenemeyecektir/ okunamayacaktır.

Signal kendiliğinden bir PİN veya şifre korumayla gelir. Bunu açın ve Signal erişmek için spesifik bir PİN kodu belirleyin (Ayarlar > Gizlilik). Mesajlar için bu ayarları (Ayarlar < SMS ve MMS > WiFi Aramaları etkinleştir) yoluyla yapabilirsiniz. Son olarak ayarlara tekrar girin ve Sohbetler ve Medya'da 'Eski mesajları sil' kısmına girin, ve bu işlem için bir süre belirleyin (örneğin en yakın tarihli aldığınız 5 mesajdan öncesini otomatik olarak silmek).

Bir mesajlaşma başlattığınızda, sağ üst köşeye tıkladığınızda burada Kaybolan mesajlar için bir seçenek göreceksiniz. Buraya tıklayın ve bir zamanlayıcı seçin. Bunun anlamı gönderilen/alınan her mesajın belirli bir süre sonunda silineceğidir (okunduktan sonraki sürede).

Mesajlaşmada, SMS'te ve telefonla aramada 'Uçtan uça' şifreleme kullanırken hem sizin hem de karşınızdakinin Signal Private Messenger yüklemiş olması gerekir. Bu nedenle programı yüklediğinizden

emin olun ve iş arkadaşlarınızın, ortaklarınızın ve arkadaşlarınızın da aynı işlemi gerçekleştirmesini sağlayın. Herhangi bir IMSI yakalayıcı normal telefon sinyallerinizin şifresini çözse dahi bu durumda güvende olacaksınız, çünkü bu program kendi "uçtan uça" şifreleme sistemini kullanmaktadır

MESAJLAŞMA



Signal Private Messenger'a ek olarak Telegram yüklemenizi öneriyoruz. Telegram normal bir chat programı gibi çalışabilir (normal şifrelemeyle) ama aynı zamanda Gizli Mesajlaşma denilen fonksiyonlara da sahiptir. Gizli mesajlaşma kullanıyorsanız, mesajlarınız uçtan uça şifrelenir ve gönderilen/alınan her mesaj için otomatik silme zamanlayıcısı belirleyebilirsiniz.

Daha önceden belirtildiği gibi mesajlaşma geçmişlerinin otomatik olarak silinmesi (yok edilmesi), güvenliğinizi için anahtar niteliktedir (62). Hatta bu gelişmiş şifrelemeden daha da önemlidir zira arkadaşınızda hiçbir iz veya bilgi bırakmaz ve böylelikle başkalarının bu verileri çalmasını/size karşı kullanmasını engellemiş olur.



Yeni Grup



Yeni Gizli Sohbet



Yeni Kanal

SÖRF, TOR VE VPN'LER



Android'de en güvenli şekilde sörf yapmanın en kolay yolu *Guardian Project's Orbot'u* veya OrFox'u kullanmanızdır. Orbot, Android için TOR'dur ve cihazınızda TOR'u başlatan uygulamadır. Ayarlar bölümünde hangi

uygulamaların TOR ile yönlendirileceğini (yani hangi uygulamaların TOR bağlantısı yoluyla internete bağlanacağını) seçebilirsiniz. İsterseniz tüm uygulamalar için bu seçeneği kullanabilirsiniz. Bunun ardından herhangi bir tarayıcı başlatıp TOR'un bağlantısıyla internette gezinebilirsiniz.



Kişiler



Saved Messages



Aramalar



Arkadaşlarını Davet Et



Ayarlar



Telegram FAQ



OrFox, spesifik olarak Orbot/TOR kullanacak

62

şekilde tasarlanmış bir tarayıcı uygulamasıdır. OrFox'u başlattığınızda bu tarayıcı internete otomatik olarak TOR yoluyla bağlanır ve başka bir şey yapmanıza gerek yoktur. Fakat bu durumda sadece OrFox tarayıcınız TOR'u kullanacaktır, diğer tüm bağlantılılar normal kalacaktır. Eğer OrFox kullanacaksanız, internette gezinmeden önce ayarlar bölümüne gidin, Gizlilik'i seçin ve Kişisel verileri temizle'ye tıklayın ve buradaki ter türlü veriyi seçerek silin. Bu işlemi OrFox'u kapattıktan sonra da gerçekleştirin. Bu yolla uygulamayla işiniz bittiğinde internet kullanımınızın ardından kalan tüm izler silinecektir.

Eğer sörf için başka tarayıcılar kullanacaksanız, telefonun kendisine ait tarayıcıları kullanmamanızı şiddetle tavsiye ediyoruz. Bu tarayıcıları mutlaka silin, eğer silmek mümkün değilse devre dışı bırakın ve ardından Opera, Chrome veya Firefox gibi daha uygun bir tarayıcı indirin. Bilgisayarınızda yaptığınız gibi ayarlar bölümüne girin ve hiçbir şifrenin otomatik olarak kaydedilmediğinden, formların otomatik doldurma özelliğinin devre dışı bırakıldığından (vb.) emin olun. Ayrıca İzleme (Do Not Track) özelliğini açın ve tarayıcınızla işiniz bittiğinde, tarayıcı geçmişini Temizle'ye tıklayarak silmeyi unutmayın.

Telefonunuzu veya telefonunuzun tarayıcısını işleriniz (e-postalarınız, bulut belleğiniz vb.) için kullanmamayı unutmayın. Bu işlere asla ve asla telefonunuzla erişmeye çalışmayın. Telefonunuzda bir veriyi tamamen silmek mümkün olmayabilir.

METADATA

Metadata hakkındaki geçmiş bölümlerle açıklandığı üzere, bu verilerin toplanması çoğunlukla telefonlar için çok daha kötü bir durumdur, zira fotoğraflarınız konumunuzu ve fotoğrafta bulunan başka kişilerin isim etiketlerini taşıyabilir. Bu nedente ister Android ister iOS kullanın, telefonunuzun kamerasıyla çektiğiniz fotoğrafları sosyal medyada paylaşmadan, belgelerinizde kullanmak için bilgisayarınıza aktarmadan veya yayınlamadan önce bir dakika düşünün. Telefon uygulamalarında metadata programları çoğunlukla *Exif* veya *Exif veri* terimlerini kullanırlar (*Exchangeable image file format – Değiştirilebilir görüntü dosyası formatı*).

Eğer bilgisayarınızla fotoğraflar çekiyorsanız, önceden gösterdiğimiz yöntemleri kullanarak bilgisayarınızdaki metadata'yı temizleyebilirsiniz. Fakat telefonunuzdan bir veriyi doğrudan yayınlamak istiyorsanız, öncelikle bir metadata temizleyici program yüklemeniz gerekmektedir.

Android için *Exif Eraser* veya *Metadata remover* programlarını kullanmanızı öneriyoruz. Bu iki programı da kullanmak kolaydır. Bunların haricinde de bir çok seçeneğinizin bulunduğunu belirtelim: iOS telefonlar için *Photo Investigator* veya *Metapho* yine önerdiğimiz programlardır. Bunları yükleyin ve test edin, nasıl çalıştıklarını anladığınızdan emin olun. Eğer emin olamıyorsanız başka bir programı deneyin ve programa ne kadar hakim olduğunu görmeye çalışın. Neredeyse tüm programların kullanma talimatları online olarak bulunabilir.

UYGULAMALAR

Yukarıda bahsettiğimiz *The Guardian Project*, bir kaç başka güvenlik uygulaması daha üretmektedir



Bunlardan biri *ChatSecure*'dur. Hem Android'de hem de iOS'ta mesajlaşmalarınızı yönetmeniz/kullanmanız için tasarlanmıştır. *ChatSecure*'u kullanarak *GoogleTalk/Chat* gibi programları güçlü şifrelemelerle kullanabilirsiniz ve bunların otomatik olarak TOR'la başlamasını sağlayabilirsiniz. Bu yolla oturumunuzdaki herhangi bir haberleşme/iletişim girişimi TOR bağlantısıyla yapılacaktır. Ayrıca programı korumak için PIN veya şifre kullanabilir, mesajlarınızın otomatik olarak silinmesini sağlayabilirsiniz.



Guardian Project'e ait bir başka popüler uygulama da *ObscuraCam*'dir. Bu bir kamera uygulamasıdır: Çektiğiniz fotoğraflardaki insanları tespit eder, yüzlerini flulaştırır (blurring) ve böylelikle başkalarının bu kişilerin yüzlerini tanımalarının önüne geçer. Ayrıca varolan fotoğraflarınızdaki yüzleri flulaştırma özelliği de vardır. *Guardian Project*'in bir çok konuda güvenlik sağlayan uygulaması mevcuttur, bu nedenle websitelerine uğrayıp bir göz atmanızda fayda var.



Eğer telefonunuzun kullandığı baz istasyonları hakkında daha nitelikli bir fikre sahip olmak ve bir IMSI yakalayıcıya yönlendirildiğiniz şüphesi doğduğunda uyarılmak istiyorsanız, Android için (iOS için ne yazık ki böyle bir program yok) *AIMSICD*'yi kullanabilirsiniz. Bu program yalnız İngilizce'dir ve Türkçe bir sürüm ne yazık ki

bulunmamaktadır. Ayrıca programı aşağıdaki linkten indirebilirsiniz:

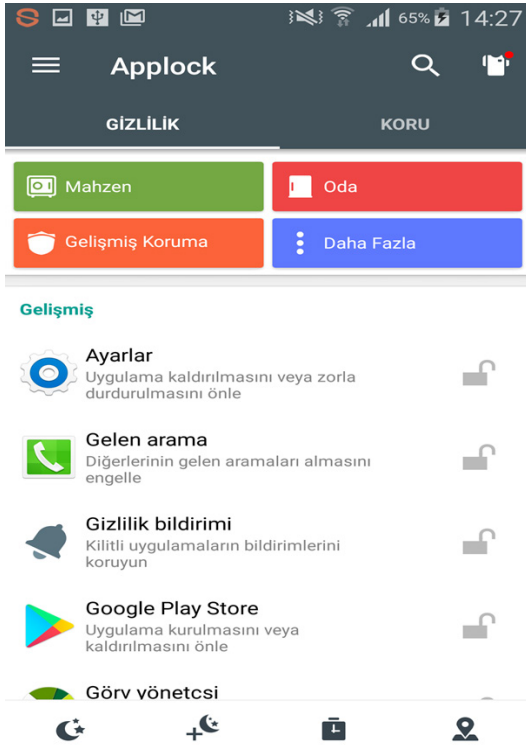
<https://github.com/CellularPrivacy/Android-IMSI-Catcher-Detector/releases>

İndirme işlemi manuel olacaktır ve ardından yüklemeyi sizin başlatmanız gerekmektedir. Ayarlar'a gidip Bilinmeyen Kaynaklara İzin Ver kısmını değiştirmeniz gerekecektir. Yükleme tamamlandığında Ayarlar'a tekrar gidip Bilinmeyen Kaynaklara İzin Ver kısmını eski haline döndürün. Program telefonunuzun bağlı olduğu baz istasyonları hakkında size bilgi sunar ve telefonunuzun bir IMSI yakalayıcıya bağlandığından şüphelendiğinde sizi uyarır. Ayrıca etrafınızdaki baz istasyonlarını gösteren bir harita fonksiyonu da vardır.

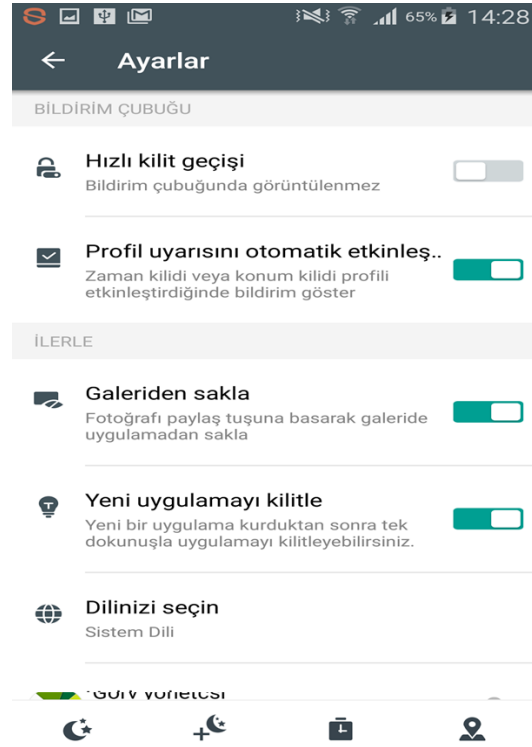


AppLock hem Türkçe hem de İngilizce arayüze sahiptir. Size bir PİN kodu yaratma ve bunu istediğiniz bir uygulamaya atama şansı verir. Bununla istediğiniz uygulamayı veya fonksiyonu PİN koduyla koruyabilirsiniz. Programın kendisi gizlidir; böylelikle başkaları sizin bu programı kullandığınızı kolaylıkla anlayamaz. Bütün uygulamalarınız için tek bir PİN kodu (veya şekli) kullanır, yani seçtiğiniz tüm uygulamalara erişim için aynı PİN kodunu kullanırsınız (63).

AppLock'u yükledikten sonra sizden bir destek programı yüklemenizi isteyecektir. AppLock'u daha fazla seçenikle kullanmanıza yarayan bu program Advanced System Protection'dır. Bunu yükleyerek AppLock için bir şifre yaratırsınız. Bu işlem ayrıca programın kendisini de saklayacak ve başkalarının bu şifreye sahip olmadan programı silmelerini imkansız kılacaktır (64).



63



64

Yükleme tamamlandığında uygulamayı nerelerde kullanacağınıza dair biraz fikir edinmek için programı kurcalayın. Uygulamanın iki sekmesi vardır: Gizlilik size korumak istediğiniz fonksiyonları ve uygulamaları seçme şansı verirken, Koruma bazı ayarları değiştirmenize, örneğin bir PİN veya şekil kullanmanıza, AppLock saklamanıza (vb.) imkan verir. Eğer uygulamayı saklamayı seçerseniz, ileride uygulamayı başlatmak için tuş ekranını açıp (tıpkı telefonunuzla bir arama yapar gibi) buraya #1234 yazıp, Ara tuşuna

basmanız gerekecektir. Bu uygulamayı başlatır. Eğer *Advanced Protection* otomatik olarak yüklenmediyse, Koruma sekmesi altında *Advanced Protection'ı etkinleştir'e* tıklayın.

iOS için Apple Uygulama Mağazasında benzer uygulamalar mevcuttur; Locker Lite bunlardan biridir fakat dil ihtiyaçlarınıza göre başkalarını da bulabilirsiniz.

KULLANIMINIZLA

Daha önceden tekrar tekrar bahsedildiği üzere, bilgisayarınızla telefonunuzun kullanımını birbirinden ayırmanız önemlidir. Genel olarak telefon bazlı uygulamaları bilgisayarınızda kullanmamanızı öneriyoruz. Örneğin Telegram'ın Windows için bir uygulaması vardır ve bu yolla programı doğrudan bilgisayarınız aracılığıyla kullanabilirsiniz. Fakat bilgisayar temelli sürüm Gizli Mesajlaşma'ya izin vermemektedir ve şifreyle korunamaz. Benzer olarak başka uygulamaların da bilgisayarınız için sürümleri olabilir fakat kullanmanızı önermiyoruz. SMS trafiğini yönetmek, mesajlarınızı okumak, mesaj yazmak gibi işler için benzer bilgisayar programları da mevcuttur ama tekrar ettiğimiz üzere, lütfen bunlardan kaçınınız.

Bunlardan muaf tek örnek Signal Private Messenger'dır. Hem Win10'da hem OSX'te çalışabildiği gibi Kaybolan Mesajlar (otomatik silme) özelliğini de korur. Bu özelliği grup mesajlaşmaları için de yapabilirsiniz. Fakat bu tip Kaybolan Mesajlar'a sahip bir konuşmayı öncelikle telefonda başlatmanız gerekmektedir, bilgisayar programı bu özelliği desteklememektedir. Telefonda başlattıktan sonra bu konuşmaları bilgisayarınızdan yapabilir ve yönetebilirsiniz.

Telefonunuzu korumanın ne kadar güç olduğunu bilmenize rağmen yine de tarayıcınızda bir araştırma yapmanız, e-mail'inize ulaşmanız veya telefonunuzu dosya/veri depolamak/taşımak için kullanmanız gerekirse, aşağıdaki önlemleri alın. Tarayıcının kullanılması durumunda öncelikle tarayıcının Ayarlar bölümüne gidip hiçbir şifrenin kaydedilmediğinden, otomatik doldurma (formlar, boşluklar için) fonksiyonun kullanımda olmadığından emin olun ve tarayıcıyı kapattıktan sonra tarayıcıda 'kişisel verileri temizle' işlemini gerçekleştirin.

Eğer telefonunuzda herhangi bir dosya/veri depoladıysanız, boş alan silen bir program yükleyin ve programı bu dosyaları sildikten/kaldırdıktan sonra çalıştırın. Bu programlar ne yazık ki telefonlarda bilgisayarlardaki kadar iyi çalışmamaktadır. Fakat yine de dosyanın geri dönüşümünü zorlaştıracaktırlar. Android'ler için Secure Eraser, iOS'lar içinse iShredder (Sadece İngilizce mevcuttur) tavsiye ettiğimiz programlardır. Bir çok benzer uygulama da mağazalarda mevcuttur. Eğer telefonunuzun bir SD kartı varsa, SD kartınızda da 'boş alan temizleme' işlemini gerçekleştirin. Ayrıca telefonun kendi belleği için de bunu yapmanızı öneriyoruz.

UNSURLAR:

- Telefonunuzdan fotoğraf veya bir veri yayınlamadan önce, dosya içerisinde hangi Metadata'ların bulunduğunu öğrenin.
- Güvenli mesajlaşma programlarınızın otomatik olarak mesajlaşma geçmişlerinizi sildiğinden emin olun ve otomatik silme kullanmadığınız fonksiyonlar varsa, konuşmayı tamamladıktan sonra mesaj geçmişinizi sildiğinizden emin olun.
- Signal'i varsayılan SMS programınız olarak kullandığınızdan emin olun ve Signal'i hem SMS hem de telefon aramaları için kullanın.

BÖLÜM 4

ENGELLEYİCİ

GÜVENLİK



PRATİK DİJİTAL GÜVENLİK

ALT BÖLÜM 12

ENGELLEYİCİ

KORUMA



Eğer bu satırları okuyorsanız, şu anda veya gelecekte güvenliğinize dair çeşitli risklerle karşı karşıya kalabileceğinizin farkındasınız. Bu riskler ne kadar küçük olurlarsa olsunlar, göz ardı edilmemelidirler. Aşağıdaki maddelere bir göz atın ve size önerdiğimiz eylemleri gerçekleştirin: İnanın 15 dakikadan fazla vaktinizi almayacak. Bu maddeler gelecekte güvenliğinizi sağlamakta önemli rollere sahip olabilirler.

Aşağıdaki Kontrol Listesi'ne dayanarak, size talimat edilen tüm bilgileri (ve isterseniz daha fazlasını) içeren bir belge oluşturun.

Yazmaya başlamadan önce kendi durumunuzu analiz etmeniz ve güvenlik sorunları yaşadığınız takdirde ne gibi desteklere ihtiyacınız olacağına karar vermeniz gerekmektedir. Bu nedenle lütfen aşağıdaki üç maddeyi gözden geçirin.

ADIM 1: KARŞI KARŞIYA OLASI VE/VEYA SENARYOLAR?

Karşı karşıya kalabileceğiniz potansiyel tehditlerin ve bunların olası gerekçelerinin tiplerini taslak haline getirin. Örneğin bir gazeteciyseniz, üzerinde çalıştığınız hikayeye mani olmak için elinizdeki malzemelere el konulması muhtemel mi? Yoksa işinizi yapmanıza toptan engel olacak ihtimallerle mi karşı karşıyasınız?

Farklı senaryolar farklı hazırlıklar gerektirebilir. İşinizde güvenliğinize risk teşkil edebilecek ne gibi çalışmalar yapmış, ne gibi insanlarla çalışmış olabilirsiniz? Yerel yolsuzluklar üzerine bir rapor mu hazırladınız? Zorlu bir mahkeme sürecinde işkence mağduru birini mi savundunuz? Güvenliğinize dair olası tehditleri içerebilecek olan bu olayları listeledikten sonra, bu tehditlerin olası kaynaklarını tanımlamanız gerekmektedir. Bu tehditin kaynağına dair hali hazırda bir fikriniz var mı? Size karşı bu eylemler gerçekleştirilirse olası yöntemi ve sonucu ne olabilir? Bu sorulara vereceğiniz cevapları olabildiğince net şekilde vermeye çalışın. Bu yolla size sağlanabilecek desteğin en hızlı şekilde gerçekleştirilmesini sağlayabilirsiniz.

ADIM 2: NE DESTEK?

Yukarıda listelediğiniz farklı olasılıklara dayanarak, ne gibi bir desteğe ihtiyaç duyacağınızı düşünüyorsunuz? Örneğin spesifik bir senaryo için uluslararası medyanın ilgisinin işlevli olacağını mı düşünüyorsunuz? Eğer cevabınız evetse, bunu listeye eklemeli ve böyle bir desteği hangi şekilde talep ettiğinizi belirtmelisiniz (örneğin alıkonulduğunuz durum bir hafta boyunca değişmezse basında yer almak mı istiyorsunuz? Veya sadece yerel kaynakların/sosyal medyanın ilgisini mi talep ediyorsunuz? Unutmamanız gereken bu konudaki farklı yaklaşımların duruma göre farklı faydaları olabilir. Bu konuda

güvendiğiniz iş arkadaşlarınızla seçeneklerinizi konuşmanız iyi olabilir, zira bu kişiler sizin lehinize/ vekaletinizle konuşacak kişiler olabilir.) Başka ne biçimde desteklere ihtiyaç duyuyorsunuz?

Uzun süreli alıkonulma, yaşamanız durumunda bakmakla, desteklemekle yükümlü olduğunuz aile bireyleriniz veya dostlarınız var mı? Bu kişiler sizden ne şekilde destek alıyorlar; tıbbi mi, finansal mı, barınma amaçlı mı?

Aynı şekilde bu gibi olaylarla karşı karşıya kaldığınızda hukuki desteğe mi ihtiyaç duyacağınızı düşünüyorsunuz? Yoksa bir takım spesifik yasal koşullara mı sahipsiniz? Temsil edileceğiniz avukatınızı seçme hakkını reddedeceğiniz herhangi bir durum olabilir mi? Hali hazırda sizin temsil edeceğine dair söz vermiş bir avukatınız var mı? Eğer varsa, bu kişi kimdir ve onunla nasıl iletişim kurulabilir?

Eğer bu örnekler sizin kararlarınızı yansıtıyorsa; hiçbir şart altında devletin atadığı bir avukat tarafından temsil edilmek istemediğinizi, bu temsiliyeti sizin seçtiğiniz bir avukatın gerçekleştireceğini açıkça belirten özel bir not/dilekçe hazırlamanız ve bunun bir kaç kopyasını çevrenizde güvendiğiniz arkadaşlarınıza veya çalışma ortaklarınıza bırakmanız faydalı olabilir

ADIM 3: ALTINDA OLMAYAN

Güvenliğiniz için belirleyeceğiniz kişi, yukarıda belirttiğimiz bilgilere sahip olan ve olası durumlarda bu bilgileri ilgili kişilerle paylaşma sorumluluğunu almış olan kişidir. Yukarıda belirttiğimiz tüm bilgilerin bu kişide bulunması gereklidir. Aynı zamanda olası bir durumda bu bilgilerle ne yapması gerektiğine dair de bu kişinin önden bilgilendirilmesi önemlidir.

Gerekli durumlarda sizin adınıza çeşitli işleri gerçekleştirebilecek bir aile bireyine (örneğin avukat bulmak) vekalet vermeyi de ihmal etmeyin. Fakat bu konuyu etraflıca düşünün: Aile bireyleriniz böyle bir sorumluluğun gerekliliklerini veya sonuçlarını gözetmeden gönüllü olabilirler. Ayrıca bu tip sorumlulukların vekalet sahipleri için yıpratıcı, stresli ve yorucu olabileceğini seçtiğiniz kişilerle konuşmayı, tartışmayı ve bu konuda tamamen rıza sahibi olduklarından emin olmayı unutmayın. İşinizi ve çalışma koşullarınızı anlayan birini seçin ve bu kişiye onu neden seçtiğinizi etraflıca anlatın. Birden fazla kişiyi güvenliğiniz için seçtiyseniz, bu kişilerin birbirinden haberdar olduğundan veya tanıştıklarından emin olun. Eğer tanışıklıkları yoksa, bu kişilerin gerekli iletişim bilgilerini birbirlerine ulaştırın.

Aşağıdaki liste, bu belgeye neleri eklemeniz gerektiğine dair size bir örnek niteliğindedir. Hangilerine ihtiyaç duyacağınıza, belgede hangilerinin bulunmasının faydalı olacağına sizin karar vermeniz daha sağlıklı olacaktır.

KONTROL LİSTESİ

- CV veya bir özgeçmiş
- Sizi ve işinizi tanıtan bir özet: Güvenliğinize dair risk teşkil edebileceğini düşündüğünüz spesifik çalışmalarınızı, bunların tarihlerini buraya eklemeye çalışın. (Bu kısmı atlamayın; burada listeleyeceğiniz çalışmalardan dolayı alıkonulmanız durumunda çalışma alanınızın hak savunuculuğuna veya sivil topluma dair olduğunu bu belge yoluyla kanıtlayma imkanına sahip olabilirsiniz.)
- Sizi temsil etmesi için belirlediğiniz yetkili avukatın iletişim bilgileri (tercihen bu kişiye dair ufak bir tanıtım yazısı)
- Acil durumda iletişim kurulacak kişilerin (güvenliğinizi için belirlediğiniz kişiler) iletişim bilgileri (tercihen bu kişilere dair ufak bir tanıtım yazısı)
- Vekalet aile bireylerinizin iletişim bilgileri (tercihen bu kişilere dair ufak bir tanıtım yazısı)
- İlgili arkadaşlarınızın veya aile bireylerinizin iletişim adresleri (tercihen bu kişilere dair ufak bir tanıtım yazısı)
- Tanıdığınız veya bu süreçte size destek olabileceğini düşündüğünüz gazetecilerin, aktivistlerin, sivil toplum çalışanlarının veya politikacıların iletişim bilgileri (tercihen bu kişilere dair ufak bir tanıtım yazısı)
- İlgili çalışma arkadaşlarınıza ve/veya iş ortaklarınıza dair iletişim bilgilerini de içeren kısa bir özet (Bu bilgiler engelleyici korumada veya tehdit tespitinde başkalarına yardımcı olabileceğinden önemlidir.)
- Kamu/medya desteğine ihtiyaç duyacağınız durumlarda kullanılmak üzere bir kaç fotoğraf da ekleyin. Bu sayede temsil edilme biçiminiz üzerinde ufak da olsa bir kontrol sahibi olabilirsiniz.

ÖNCEDEN MALZEMELER

Sizin tarafından önceden düzenlenmiş malzemeler, alıkonulma gibi bir durumla karşı karşıya kaldığınızda paylaşılacak olan malzemelerdir (bu malzemelerin ne zaman/nasıl/ne koşullar altında paylaşılmasını istediğinizi eklemeyi ihmal etmeyin.). Aşağıdaki örneğe göz atın. Bazen ufak videolar hazırlamak fazlasıyla faydalı olabilir.

Önceden hazırlanmış malzemenin açıklaması: Bu malzemelerin ne olacağına karar vermek tamamen size bağlıdır. Bunları belirlerken işinizi ve hayal edebildiğiniz tehditleri baz alın. Örneğin;

- Günümüzde zorla itiraf alma git gide daha yaygın hale gelmektedir. İsveç vatandaşı olan Gui Minhai, Tayland'da alıkonularak Çin'e kaçırılmıştır. Zorla alınan itirafında İsveç'ten hiçbir diplomatik yardım talep etmemesi istenmiş ve açıklamasında İsveç vatandaşlığından feragat ettiğini beyan etmiştir. Minhai'nin önceden kendi kaydettiği bir video hayal edin; videoda günün birinde Çin'de ortaya çıkması halinde kaçırılmış olduğunu (zira Minhai Çin'de ortaya çıktığında, Çin'e girişi için gerekli vizeye ve evraklara sahip değildi) veya hiçbir durum altında İsveç vatandaşlığından vazgeçmeyeceğini, diplomatik yardımı reddetmeyeceğini belirten bir açıklama yaptığını düşünün. Bu video (malzeme) zorla verilmiş gerçek dışı bir itirafa karşı çok güçlü bir kanıt teşkil edebilirdi. Videonun varlığı bu davaya olan ilgiyi güçlendirebilir ve Minhai'ye yardımın/desteğin sınırlarını genişletebilirdi.
- Bazı hak savunucularının aile bireyleriyle, ziyaretçilerle veya avukatlarıyla görüşme hakları ellerinden alınabilir. Hatta bazen yetkililer bu kişilerin avukat haklarından feragat ettiklerini, bunun yerine devlet tarafından atanmış bir avukatı tercih ettiklerini beyan edebilirler. Benzer biçimde bu duruma maruz kalan kişinin, ardında açıkça avukat hakkından asla feragat etmeyeceğini, hiçbir avukatı kabul etmeyeceğini belirttiği ve

önceden hazırlayıp gerekli kişilere birer nüshasını bıraktığı bir dilekçenin var olduğunu düşünün.

- Üçüncü kişilerin, çalışmalarınızın çeşitli bölümlerini size karşı kullanabileceğini düşünüyorsanız, bu çalışmaların ne olduğunu ve neden tamamen yasal bir çerçeveye sahip olduğunu anlattığınız önceden kaydedilmiş bir video hazırladığınızı düşünün. Daha önceden çalışmalarınız yüzünden tehdit edildiyse, uyarıldıysanız, korkutulmaya çalışıldıysanız, videoda bunlara değinmeniz size çeşitli açılardan fayda sunabilir.
- Üçüncü kişilerin size STK çalışmalarınızdan ötürü yasa dışı iş yapmakla suçlama ihtimali olduğunu mu düşünüyorsunuz? Veya bu çalışmalar üzerinden finansal suistimal veya dolandırıcılıkla suçlanma ihtimalini mi gözetiyorsunuz? Bu durumda çalışmalarınızın ekonomik raporlarının, vergi işlemlerinin veya ilgili belgelerinin güvenliğinizi için seçtiğiniz kişiye birer kopyasını ulaştırın. Bu sayede suçlamaları savuşturmanız mümkün olabilir.

ÖNEMLİ: Hazırlayacağınız bu malzemeleri güncellemeyi unutmayın: Adresinizin değişmesi, acil iletişim kurulacak kişilerdeki değişiklikler, işinizin, aile durumunuzun değişimi mutlaka bu belgelerde güncel olmalıdır. Güncellediğiniz belgeleri tekrar ilgili kişilere yenilenmiş haliyle göndermeyi sakın unutmayın.