Cihazlarınızın güvenliğini sağlama

Şu anda okumakta olduğunuz kaynak, cihazları yaygın cihaz izleme biçimlerine karşı korumak için bazı pratik ilk adımlar sunmaktadır. Farklı eylemleri kapsar: Bluetooth, WiFi ve konum paylaşımını kapatma; aygıtınızı yeniden adlandırma; casus yazılım ve uygulama izinlerini kontrol etme; fabrika ayarlarına sıfırlama.

Bunlar cihaz(lar)ınızı nasıl güvende tutacağınıza dair genel ipuçlarıdır. Kesin adımlar farklı cihazlar için farklı olabilir, ayrıca zaman içinde değişebilir.

iPhone ve iPad'lerde, genellikle Ana Ekranda "Ayarlar"a dokunarak ve ardından arama çubuğunu göstermek için aşağı kaydırarak bir ayar bulabilirsiniz (Yardım için http://tiny.cc/iphonesearch adresini ziyaret edin.)

Android cihazlarda Ana Ekrandan yukarı kaydırın: "Telefonunuzda ve Daha Fazlasında Arama Yapın" yazan bir arama çubuğu görünecektir. Arama çubuğuna aradığınız ayarı yazın.

Kullanmadığınız zamanlarda Bluetooth ve WiFi'ı kapatma

Etkinleştirilmiş Bluetooth ve WiFi, cihazınızı diğer cihazlara görünür hale getirir İhtiyacınız yok mu? Onları kapatın **Ayarlar** a gidin veya **Bluetooth** ve **WiFi** simgelerine dokunun.

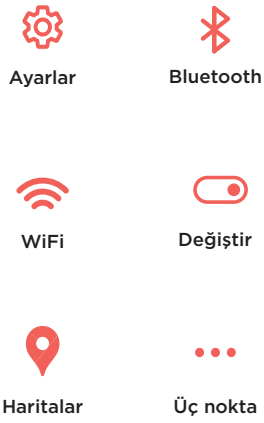
Ek olarak, bluetooth ayarlarınıza gidebilir (**Ayarlar > Bluetooth**) ve akıllı telefonunuzla eşleştirilmiş tüm cihazlara göz atabilirsiniz. Tanınmayan herhangi bir cihaz bulursanız, eşleştirmeyi kaldırın.

Konum paylaşımını kapatın

Konum paylaşımı ve "Telefonumu Bul" gibi uygulamalar telefonunuz kapalıyken de çalışır, bu nedenle ayarlardan kapatmanız gerekir. iPhone'da **Ayarlar** > Gizlilik > Konum Servisleri'ni açın veya "Konum Servisleri "ni arayın ve buradan konum paylaşımını kapatın.

Bir Android cihazda, **Haritaları** açın, profil resminize ve ardından Konum paylaşımına dokunun. *Konumunuzu görmemesi gereken* herhangi birinin profil resmine dokunun, ardından "Durdur"a dokunun.

Simge ve anahtar



©2023 MediaSmarts

Cihazlarınızın güvenliğini sağlama

Aygıtlarınızı yeniden adlandırma

Telefonunuzun adını hiç değiştirmemiş olsanız bile, hala tanımlayıcı olarak hizmet veren bir adı vardır. iPhone aygıtında: **Ayarlar** > Genel > Hakkında > Ad öğesine dokunun veya "Ad" öğesini arayın, ardından yeni bir ad girin ve "Bitti" öğesine dokunun.

Android cihazda: **Ayarlar** Ayarlar > Telefon hakkında > Cihaz adı'na dokunun veya "Ad" için arama yapın, ardından yeni adı yazın ve "Tamam "a dokunun.

Casus yazılımları kontrol edin

"Casus yazılım", başka birinin cihazınızı gözetlemesine izin veren uygulamalar anlamına gelir Tanımadığınız herhangi bir uygulama olup olmadığını kontrol edin. iPhone aygıtında, yazılım kitaplığını görene kadar Ana ekranda sağa kaydırın.

Ekranın üst kısmındaki arama kutusuna dokunun, ardından uygulamalar listesinde ilerleyin ve tanımadığınız her şeyi kaldırın.

Android cihazda, **Ayarlar** > Uygulamalar ve bildirimler > Tüm uygulamaları gör bölümüne gidin veya "Uygulamalar "ı arayın.

Cihazlarınızı casus yazılımlara karşı tarayan *Certo* ve *Incognito* gibi uygulamalar da vardır; ancak, casus yazılımların telefonunuzda hala gizli olma ihtimalinin her zaman olduğunu bilmelisiniz.

Uygulama izinlerini kontrol edin

Ayrıca herhangi bir uygulamanın konumunuz gibi şeyleri toplamasını veya paylaşmasını da durdurabilirsiniz. iPhone'da, her bir uygulamanın ne paylaştığını görmek için **Üç nokta** > Gizlilik ve Güvenlik > Uygulama Gizlilik Raporu'na dokunun veya "Gizlilik Raporu"nu arayın. Ayarları değiştirmek için her bir uygulamaya dokunun.

Bir Android cihazda, Google Play mağazasından *DuckDuckGo* uygulamasını indirin ve ardından açın. **Ayarlar** > Uygulama İzleme Koruması öğesine dokunun ve ardından **değiştir** öğesini sağa kaydırın.

Fabrika ayarlarına sıfırlama

Diğer her şeyi yaptıysanız ve hala birinin telefonunuzu izlediğini düşünüyorsanız, fabrika ayarlarına sıfırlayabilirsiniz. Ancak bu işlem, telefonunuzdaki kanıtlar da dahil olmak üzere tüm mevcut verilerinizi silecektir. Telefonunuzu sıfırlarsanız, kayıtlı bir yedekten geri yükleme yapamazsınız. Nedeni - sizi izleyen her şey yeniden yüklenmiş olabilir: tamamen baştan başlamanız gerekir.

Bunu yapmak istediğinizden eminseniz, iPhone'da **Ayarlar** > Genel > iPhone'u Aktar veya Sıfırla'ya, ardından "Tüm İçeriği ve Ayarları Sil" seçeneğine dokunabilirsiniz. Bu ayarı bulmak için "Sıfırla" seçeneğini de arayabilirsiniz.

Bir iPhone'unuz varsa, sizi çoğu casus yazılım türünden koruyan "Kilitleme Modu "nu da etkinleştirebilirsiniz. Ayrıca FaceTime ve Safari gibi uygulamaları ne kadar kullanabileceğinizi de sınırlar. "Kilitleme Modu" hakkında daha fazla bilgi için https://support.apple.com/en-ca/HT212650 adresini ziyaret edin.

Bir Android cihazda, **Ayarlar** 'a giderek başlayın, ardından "Sıfırla "yı arayın. "Fabrika ayarlarına sıfırla" veya 'Tüm verileri sil' gibi bir sonuç arayın. Dokun ona.

Media Smarts

Financial contribution from

Public Health Agency of Canada
Agence de la santé publique du Canada

Dijital iletişimin güvenli yolu

Şu anda okumakta olduğunuz kaynak, çevrimiçi ortamda güvenli bir şekilde iletişim kurmak için bazı pratik ilk adımlar sunmaktadır. Yaygın çevrimiçi izleme biçimlerinden kaçınmayı sağlar ve hesaplardan çıkış yapma, konum paylaşımını kapatma, gizlilik ayarlarını gözden geçirme, şifreleri değiştirme gibi eylemleri kapsar.

Bunlar cihaz(lar)ınızı nasıl güvende tutacağınıza dair genel ipuçlarıdır Kesin adımlar farklı cihazlar için farklı olabilir, ayrıca zaman içinde değişebilir

iPhone ve iPad'lerde, genellikle Ana Ekranda "Ayarlar"a dokunarak ve ardından arama çubuğunu göstermek için aşağı kaydırarak bir ayar bulabilirsiniz (Yardım için http://tiny.cc/iphonesearch adresini ziyaret edin.)

android

Android cihazlarda Ana Ekrandan yukarı kaydırın: "Telefonunuzda ve Daha Fazlasında Arama Yapın" yazan bir arama çubuğu görünecektir. Arama çubuğuna aradığınız ayarı yazın.

Tüm hesaplardan çıkış yapma

Bazı uygulamalarda birden fazla cihazda oturum açmış olabilirsiniz. *Facebook*'ta her yerden nasıl çıkış yapacağınız aşağıda açıklanmıştır: **Üç nokta** ve ardından **Ayarlar**, ardından "Parola ve Güvenlik" ve ardından "Hesaplar Merkezi". "Parola ve Güvenlik" ve ardından 'Oturum Açtığınız Yer' üzerine dokunun.

Şimdi tüm *Facebook*, *Instagram* ve *WhatsApp* hesaplarınızı göreceksiniz. Onlara tek tek dokunun ve hangi cihazlarda oturum açtığınızı kontrol edin. Ardından telefonunuz olmayan her biri için "Oturumu Kapat"a dokunun.

Simge ve anahtar

Üç nokta

Ayarlar

Dikey üç nokta

Değiştir

©2023 MediaSmarts

Sosyal medyada konum paylaşımını kapatma

Bu, özellikle haritada nerede olduğunuzu gösteren *Snapchat*, kullanıyorsanız önemlidir. Bunu yapmak için *Snapchati* açın ve profil simgenize dokunun. Ardından sağ üstteki **üç dikey noktaya (eksilti)** dokunun ve "Kim Yapabilir..." bölümüne ilerleyin. "Konumumu Gör "e dokunursanız, 'Hayalet Modu' yazan bir açılır pencere belirecektir. Etkinleştirin, Açık moduna **değiştirin**.

Facebook veya *Instagram*'da konumu kapatabilirsiniz. Bunu yapmak için **Ayarlar** > Gizlilik > Konum Servisleri'ne dokunun, ardından yanlarındaki **Değiştir** 'e dokunun. Diğer sosyal ağların çoğu bunu "Gizlilik" veya "Güvenlik" gibi ayarlar içinde benzer yerlere koyar.

Gizlilik ayarlarını gözden geçirin

Tüm sosyal ağ hesaplarınızın gizlilik ayarları vardır ve bunlara genellikle **Ayarlar** 'a ve ardından "Gizlilik", "Gizlilik ve Güvenlik" veya "Kitle" gibi bir şeye dokunarak erişebilirsiniz. Yalnızca Arkadaşlarınıza gönderdiklerinizi gösterecek şekilde ayarlandığından emin olun.

Bulut depolama alanındaki parolaları değiştirme

Fotoğraflarınız veya videolarınız için *iCloud*, *Google Drive* vb. gibi herhangi bir bulut depolama alanı kullanıyorsanız, erişim şifrelerini değiştirdiğinizden ve yetkisiz kişilerin erişimini engellediğinizden emin olun.

MediaSmarts

Financial contribution from

Public Health Agency of Canada
Agence de la santé publique du Canada

Güvenli tarama

Şu anda okumakta olduğunuz kaynak, çevrimiçi ortamda güvenli bir şekilde tarama için bazı pratik ilk adımlar sunmaktadır. Yaygın çevrimiçi izleme biçimlerinden kaçınmayı sağlar. Ayrıca, gizlilik odaklı tarayıcılar kullanmak, gizli modda gezinmek, geçmişi temizlemek, anonim e-postalarla oturum açmak, güçlü parolalar kullanmak gibi eylemleri açıklar.

Bunlar cihaz(lar)ınızı nasıl güvende tutacağınıza dair genel ipuçlarıdır
Kesin adımlar farklı cihazlar için farklı olabilir, ayrıca zaman içinde değişebilir

iPhone ve iPad'lerde, genellikle Ana Ekranda "Ayarlar"a dokunarak ve ardından arama çubuğunu göstermek için aşağı kaydırarak bir ayar bulabilirsiniz (Yardım için http://tiny.cc/iphonesearch adresini ziyaret edin.)

Android cihazlarda Ana Ekrandan yukarı kaydırın: "Telefonunuzda ve Daha Fazlasında Arama Yapın" yazan bir arama çubuğu görünecektir. Arama çubuğuna aradığınız ayarı yazın.

Gizlilik odaklı bir göz atma kullanın

Firefox ve *DuckDuckGo* gibi tarayıcılar gizlilik göz önünde bulundurularak tasarlanmıştır, bu nedenle sizi mümkün olduğunca az izlerler. Cihazınızla birlikte gelen tarayıcı yerine bunlardan birini kullanmayı deneyin.

Gizli tarama

Çoğu tarayıcının **gizli modu** vardır. Bu mod, tarayıcınızın hangi siteleri ziyaret ettiğinizi kaydetmesini engeller, ancak bu sitelerin (veya internet sağlayıcınızın veya cihazınızdaki diğer uygulamaların) yaptıklarınızı kaydetmesini engellemez.

Simge ve anahtar

Gizli mod

Ayarlar

©2023 MediaSmarts

Güvenli tarama

Aktivite geçmişinizi temizleme

“Tarih” için arama yapın *Google* hesabı sahipleri için: *Google* ve *YouTube* geçmişinizi de temizleyebilirsiniz. **myactivity.google.com** adresine gidin, ardından “Web ve Uygulama Etkinliği”, “Konum Geçmişi” ve “YouTube Geçmişi” seçeneklerini kapatın.

Safari'de tarayıcı geçmişinizi temizlemek için **Ayarlar** ve ardından Safari > Geçmişi ve Web Sitesi Verilerini Temizle'ye dokunun veya “Web Sitesi Verileri”ni arayın.

Anonim bir e-posta ile oturum açın

Birçok web sitesi ve hizmet, kaydolmak için bir e-posta adresi vermenizi ister. Bir doğrulama bağlantısına tıklamanız gerekmiyorsa, **Sharklasers.com** adresinde oluşturulmuş sahte bir e-posta adresi kullanabilirsiniz.

İsteğe bağlı olarak, ücretsiz, özel ve güvenli bir *Protonmail* adresi oluşturabilir ve kullanabilirsiniz – bu şekilde başka birinin tanıyamayacağı bir adres elde edersiniz.

Güçlü parolalar kullanın

Akılda kalıcı bir cümle ile başlayarak (“I like bananas” gibi) ve ardından bazı harfleri sayılara veya karakterlere dönüştürerek (yıldız işareti veya nida işareti gibi !L1keBan@nas) güçlü bir parola oluşturabilirsiniz.

Unutmayın: farklı hesaplar için aynı şifreyi kullanmayın. Özellikle önemli: ana e-posta hesabınız için farklı ve güçlü bir parola kullanın, çünkü hesap kurtarma e-postaları oraya gönderilecektir. Bir şifre yöneticisi de kullanabilirsiniz: *1Password* veya diğer. Bunu yaparsanız, bunun için kullandığınız parolanın güçlü ve diğer tüm parolalarınızdan farklı olduğundan emin olun.

MediaSmarts

Financial contribution from

Public Health Agency of Canada
Agence de la santé publique du Canada