GÜVENLİ GÜNLER BÜLTENİ

Bilgisayar kullanıcılarına yönelik hazırlanır. Her ayın 15'i çıkar. Diğer sayılara erişmek ve sonraki mesajların direk posta kutunuza gelmesi için guvenligunler.com adresini ziyaret ediniz.

ŞUBAT 2020

En Akıllı Telefon Bende

***EN GÜNCEL** özellikleri barındıranına sahip olmak için çırpındığımız, belki de teknolojinin var olan en büyük mucizesi akıllı telefonlar hepimizin rüyası.*

Binlerce farklı cihaza ait özellikleri tek çatı altında toplayabilen bu mucizevi aletler, son yıllarda ellerimizden düşürmediğimiz, yanımızdan bir saniye ayırdığımızda eksikliğini fazlasıyla hissettiğimiz önemli bir parçamız haline geldi. Akıllı telefonumuz sabah uyanmamız için kurulan alarm, gün içinde mutlu olduğumuz anları kayıt altına alabildiğimiz kamera, ölümsüz kılmak istediğimiz anlar için kullandığımız fotoğraf makinesi, sosyal medya kullanımıyla sevdiklerimizle iletişime geçip hayatımızı paylaştığımız bir aile meclisi, internetin en ücra köşesine eriştiğimiz bir arama kaynağı; binlerce uygulamayla yeme içme dahil temel ihtiyaçlarımızın kapımıza kadar getirilmesinden, tatil, kariyer ve daha sayamadığımız hayatın içinden pek çok faaliyeti sadece parmak hareketleriyle gerçekleştirmemizi sağlayan bir aygıt. Hepimiz telefonların ne denli hayatımızın içinde olduğunun farkındayız. Aslında, size yukarıdaki bilgileri verirken akıllı telefonun ne olduğunu, ne gibi faydalar sağladığını değil, ne kadar fazla kritik bilgiyi içinde barındırdığını anlatmaya çalıştım. Bilginin, günümüzde bizler için ne kadar değerli olduğu düşünüldüğünde, akıllı cihazlarımızın barındırdığı kişisel bilgi ve veriler

konusunda farkındalık sahibi olmamız gerektiği açıkça ortaya çıkmaktadır. Çünkü teknoloji ortamının suçluları yani siber güvenlik dünyasındaki adlarıyla hacker'lar için bir başkasına ait banka şifrelerine, tehdit amaçlı kullanabilecekleri özel fotoğraf ve videolara ulaşmak en temel amaçtır.

BU TEHLİKELERİ ENGELLEMEK İÇİN NELER YAPABİLİRİZ?

» Bir an için telefonunuzun kötü niyetli bir kişi tarafından ele geçirildiğini düşünün. Ne yapmalısınız? İlk olarak, eğer telefonunuz destekliyorsa **parmak izi** veya **yüz tanıma** gibi size özel kilit açma seçeneklerini kesinlikle aktif hale getirin. Bu bir saniyelik uğraş sizi büyük kayıplardan kurtaracaktır. Bunun dışında, telefonunuza mutlaka PIN kodu ve ekran kilit kodu koymalısınız. Koyduğunuz şifrelerin birbirinden farklı olması gerektiğinin de altı çizilmelidir. Ancak böylece şifrelerinizden biri kötü niyetli kişilerce öğrenildiğinde, diğer şifreyle telefonunuzu kurtarabilirsiniz.

» Son zamanlarda bilgisayar kameralarının tehdit içerdiği bilincinin artmakta ve kameraların kapatıldığına şahit olmaktayız; aynı tehlike akıllı telefonlar için de geçerlidir. Kötü niyetli kişilerin, ele geçirdikleri telefonlarla ortam dinlemeleri ve video kaydı yaptıkları biliniyor. Şu aşamada bazı telefon kılıflarında bulunan **kamera kapatma** ve **gerektiğinde açma** özelliği bu riskin yönetilmesinde kullanılabilir.

» E-devlet ve banka uygulamaları gibi kritik kişisel veri ve mülk içeren uygulamalar öncelikli olmak üzere, hiçbir yerde **"Şifremi Hatırla"** seçeneğinin **tercih edilmemesi** çok önemlidir. Güvenliğinden şüphe duyduğunuz uygulamaları kesinlikle kullanmayın. Uygulamanın güvenliğinden emin olmak için Android veya IOS mağazalarında uygulamaların güven derecesine ve kullanım oranına göz atın. Zararlı bir yazılım içeren uygulama kullandığınızda, telefonunuzdaki tüm bilgiler tehlikeli ellere geçebilir.

» Tabii ki, telefon kullanımını anlamlı hale getiren en önemli şey hücresel veri boyutudur. İnternetimizin kaç GB kaldığını sürekli takip etmekte ve bitmesini önlemek için nerede **ücretsiz ve şifresiz bir Wi-Fi** ağı varsa, ne kadar tehlikeli olabileceğini düşünmeden, hemen bağlantı sağlıyoruz. Ancak unutmamamız gereken nokta, kimsenin bize karşılıksız internet sağlamayacağıdır. Kafeler, havalimanları ve kütüphaneler gibi ortak kullanım sağlanan yerlerde hacker'lar, ilgili kurum ağına benzer bir şekilde "Kütüphane-Wi-Fi" veya "Kahveci" gibi adlarla sizin o ağa bağlanmanızı sağlayıp kişisel verilerinizi elde etme çabasına giriyorlar. Bu nedenle bağlantı sağladığınız Wi-Fi'ların güvenilirliğinden emin olmasınız.

» Mobil cihazlar, kullanıcılar tarafından her zaman aktif tutulduğu için, bütün kimlik avı saldırılarının ön yüzünü oluşturuyor. Mobil cihazların en savunmasız teknoloji aracı olarak görülmesi sebebiyle e-postaları takip etmek çok önemli. Hacker'lar genellikle **ilgi çekici e-postalar** göndererek, hedeflerindeki kullanıcıları istedikleri dosyayı indirmeye veya bir bağlantıyı açmaya zorluyorlar. Bu gibi durumlara karşı uyanık olmak ve oltalama saldırısı olarak nitelendirilen bu durumları iyice anlamak gerekir.

» **WhatsApp** ve benzeri mesajlaşma uygulamalarında aileniz veya arkadaşlarınız tarafından gönderilen mesajların da

güvenliğini sorgulamalı ve sizin dışınızda gelişen bu indirme işlemlerinin size zarar vermesini önlemelisiniz. **Konum özelliği** ise, zorunlu durumlar dışında açık tutulmamalıdır. Uygulamaların "konumunuza erişilmek isteniyor" talebi de büyük tehdit içeriyor; zaten aksi durumlarda bu sorunun sorulması zorunlu kılınmazdı. Konum özelliğinizi ele geçiren bir hacker'ın sizi sürekli izleyeceğini ve nereye giderseniz gidin takip edebileceğini asla unutmamalısınız.

Hızına hiçbirimizin yetişemediği bu bilgi çağında tabii ki telefonlar hayatımızı çok kolaylaştırıyor, hatta gerçek anlamda bir zorunluluk haline geldi. Ancak, nasıl evimizin kapısını açık bırakıp evden çıkamıyorsak, en az evimiz kadar değerli olan bilgilerimizi barındıran telefonlarımızın güvenliğine de önem vermeliyiz. Telefon sağlayıcılar, keşfedilen bütün güvenlik açıklarına karşı önlemler alarak bu güncellemeleri telefonlarımıza uyguluyorlar. Dolayısıyla telefonumuzda her zaman en güncel yazılımın aktif olmasını sağlamalıyız. Sonrasında da, yukarıda sözü edilen temel önlemleri almalı, yani telefonumuzun kapısını dışarıdan açılmayacak biçimde kilitleyip, içinde rahat ve özgürce bu mucizenin keyfini çıkarmalıyız.

YazaR HakkıNda

TEVFİK KOR 1999 yılında İstanbul Teknik Üniversitesi Endüstri Mühendisliği bölümünden mezun olduktan sonra danışmanlık, Proje ve Müşteri Yöneticilikleri, İş Çözümleri Birimi Müdürlüğü, Telekom, Finans ve Enerji alanlarında Sektör Yöneticilikleri ve Standart Yazılım Direktörlüğü görevlerinde bulundu. Kurucu ortaklığını yaptığı Teknosis firmasında görev aldı. Son olarak SabancıDx bünyesinde Dijital Dönüşüm Direktörü görevini yürütmeye müteakip Eylül 2019 itibariyle Dijital Dönüşüm Genel Müdür Yardımcılığı görevini sürdürmektedir.