GÜVENLİ GÜNLER BÜLTENİ

Bilgisayar kullanıcılarına yönelik hazırlanır. Her ayın 15'i çıkar. Bültenlerin her ay size ulaşması için üye olunuz: http://eepurl.com/bP-tWn

MAYIS 2016

En Büyük Sırdaşımız Mobil Cihazları Korumanın 10 yolu

MOBİL CİHAZ KULLANIMI, GÜNÜMÜZÜN EN ÖNEMLİ ALIŞKANLIKLARDAN BİRİ HALİNE GELMİŞTİR. ***Peki mobil cihazlarımızla oluşabilecek riskler nelerdir?***

- ***Ortam dinlenmesi***
- ***Gizli kamerayla ortam izlenmesi***
- ***Kısa mesaj bilgilerinin çalınması***
- ***Konum bilgilerinin takibi***
- ***Arama ve aranma bilgileri***
- ***İnternet bağlantı bilgileri, kullanıcı adı ve şifreleri***
- ***Sosyal medya bilgileri***
- ***E-posta bilgileri***
- ***Rehber bilgileri***
- ***Takvim bilgileri*** [1] [2]

Sizler de, birçoğumuz gibi artık bankacılık ve uçak bileti işlemleriniz ile otel rezervasyonlarınızı mobil cihazlardan gerçekleştiriyor; kişisel notlarınızı, parolalarınızı ve fotoğraflarınızı mobil cihazlarınızda saklıyorsanız, aşağıda belirteceğim önlemleri almanızı tavsiye ederim. [3]

Ekran koruyucu şifresi kullanın

Basit ancak kesinlikle kullanılması gereken bir önlemdir; telefonunuz yanınızda olmadığında, kaybettiğinizde veya farklı kişilerin erişim sağlaması durumunda e-postalarınıza, resimlerinize ve rehberinize erişimi engelleyecek ilk önlem, ekran koruyucusu şifrenizdir.

Güvenlik ayarlarını bilinçsizce değiştirmeyin

Kullanmış olduğumuz telefonlarda bazı temel güvenlik ayarları fabrika çıkışında yapılandırılarak bize gönderilir. Bunlar işletim sistemi seviyesinde önemli noktalara erişimi kısıtlayan ve kullanıcının güvenliğini sağlayan ayarlardır. Bu ayarların değiştirilmesi durumunda Iphone telefonlar için jail break, Android telefonlar için rooting işleminin yapılmasının önü açılır ve kötü niyetli kişiler telefondaki tüm bilgilere erişim sağlayabilir.

Sadece güvenilir kaynaklardan uygulama indirin

IOS ve Android işletim sistemi kullanan cihazlar özel bir yapılandırma bulunmaması durumunda sadece kendi marketlerinden uygulama indirebilirler, bu marketteki uygulamalar belli denetimlerden geçerek markete yüklendiği için temelde güvenli kabul edilir. Bu nedenle Android ve IOS cihazlar için kendi marketleri dışında uygulama yüklenmesi tavsiye edilmez.

Özellikle Android marketten yüklenen bazı uygulamalar zararlı yazılım içerebilmektedir, bu nedenle yüklenecek uygulamanın internet üzerinden kısaca araştırılması, oylama puanına bakılması ve uygulama yorumlarının incelenmesi oldukça yararlı olacaktır.

Talep edilen yetkilere dikkat edin

Herhangi bir uygulamayı telefonunuza kurmak istediğinizde, sizden bazı erişim yetkileri istenir; bu uygulamanın gerçekten bu yetkilere sahip olması gerekip gerekmediğini değerlendirin ve ancak gerekli ise kuruluma devam edin.

Örneğin her hangi bir e-ticaret sitesine ait uygulama sizin galerinize veya rehberinize erişmek istiyorsa, bu durumu bir kez daha değerlendirin.

Güncellemelerinizi kontrol edin ve düzenli olarak yükleyin

İşletim sistemleri için yayınlanan güncellemeler genellikle işletim sistemindeki yazılım kaynaklı bir sorunu düzeltme veya herhangi bir güvenlik riskini ortadan kaldırma amacıyla yayınlanır; bu nedenle güncellemelerinizi düzenli olarak takip edin ve yükleyin.

Düzenli olarak yedek alın

Telefonunuzun kullanmış olduğu işletim sisteminin bozulması, virüs bulaşması veya telefonunuzun fiziksel olarak bozulması sonucunda telefonunuzdaki dosya ve diğer bilgilere erişiminiz mümkün olmayabilir; bu nedenle önemli dosya ve bilgilerinizi düzenli olarak yedekleyin. Bu işlemin manuel olarak yapılması çoğu zaman unutulduğu için, otomatik olarak gerçekleştiren uygulamaları tercih edin.

Kablosuz ağ kullanımı

Kamuya açık alanlarda ücretsiz olarak yayın yapan kablosuz ağları, sahibini bilmiyorsanız ve güvenliğinden emin değilseniz kesinlikle kullanmayın; kullanmak zorunda kalmanız durumunda VPN bağlantısı ile iletişimi şifreleyerek kullanın. Ancak, VPN gibi önlemlere rağmen mobil hattınıza ait interneti kullanmanız daha güvenli olacaktır.

Mobil cihazınızın uzaktan yönetilmesine izin verin

Mobil cihazınızda gerekli yapılandırmaları yapmanız durumunda cihazınızı uzaktan yönetebilir, içindeki verileri silebilir ve cihazınızın konumunu harita üzerinde görebilirsiniz. Bu özellik, kaybettiğinizde veya yetkisiz kişilerin eline geçmesi durumunda ya cihazınızı bulmanızı sağlar veya içindeki önemli verileri silmenizi olanaklı kılarak bilgilerinizin yetkisiz kişilerin eline geçmesini engeller.

Güncel güvenilir anti-virüs uygulamaları kullanın

Tıpkı bilgisayarlarda olduğu gibi telefonlara da virüs bulaşabilir ve içindeki bilgileri alabilir; bu nedenle güncel tehditlere karşı korunmak için güncel anti-virüs uygulamaları kullanmamız gerekir.

Telefonunuz çalındığında hemen BTK'ye bildirin

Çalındığından emin olduğunuz telefonlarınızı IMEI numarası ile BTK'nin 7/24 hattı 0 (312) 294 94 94'e bildirip Türkiye GSM operatörlerinde kullanıma kapatılabilirsiniz. Telefona herhangi bir Türkiye GSM operatörünün kartı takıldığında kullanıcıya bir SMS gelir ve telefonun çalıntı olduğu bilgisi BTK'ye iletilir ve telefon hiçbir şekilde Türkiye operatörlerinde kullanılamaz. Telefonunuzun IMEI numarasını öğrenmek için *#06# yazıp arama tuşuna tıklayın. IMEI numarası ekranda belirecektir. IMEI numarasını güvenli bir şekilde saklayın. Ayrıntılı bilgi için http://mcks.gov.tr'yi inceleyebilirsiniz.

REFERANSLAR

1. Net Market Share (Nisan 2016). *'Mobile/Tablet Operating System Market Share'*. Web sayfası: https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=1.

2. Garnaeva M., Chebyshev V., Makrushin D. & Ivanov A. (Mayıs 2015). *'IT threat evolution in Q1 2015'*. Web sayfası: https://securelist.com/analysis/quarterly-malware-reports/69872/it-threat-evolution-in-q1-2015/

3. Bilgi Teknolojileri ve İletişim Kurumu. (Nisan 2016). Web sayfası: http://www.btk.gov.tr/tr-TR/Anasayfa

YAZAR HAKKINDA

Erdem Kayar, Bilgisayar Mühendisliği'nden mezun oldu. 6 yıldır Lostar firmasında Bilgi Güvenliği alanında (SCADA, Mobil, Web uygulaması, Network Tasarım, Statik Kod Analizi, PCI/DSS) çalışmalar gerçekleştiriyor. 2013 yılından beri Lostar'da Teknik Departman'ın yöneticiliğini gerçekleştiriyor.