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.

MAYIS 2018

Kim Benimle Neden Uğraşsın?

SAKLAYACAK BİR ŞEYİM DE, gizli ya da kritik bir işlemim de yok. Ne olabilir ki? Neden güvenlik önlemi almalıyım?

Internet'in hayatımıza girmesiyle akıllanan telefonlar, televizyonlar ve ev aletleri hem hayatımızı kolaylaştırıyor hem de bizi eğlendiriyor ve oyalıyorlar. Peki, sıradan bir vatandaş olarak, kim benim hayatımı ne yapsın, benimle neden uğraşsın diye düşünerek, güvenlik önlemlerini önemsemediğiniz oluyor mu? Bu yazımda, bir siber güvenlik uzmanı olarak sizlere, sık karşılaşılan, yaygın kullanılan sosyal medya uygulamalarından gündelik örnekler verecek ve güvenlik önlemlerinin öneminden bahsetmeye çalışacağım.

GÜVENLİKSİZ CİHAZLAR

Güvenliksiz bilgisayarları, üzerinde antivirüs programı olmayan, güvenlik güncellemeleri yapılmamış, lisanssız işletim sistemi çalıştıran bilgisayarlar olarak tanımlayabiliriz. Tabii bu saydıklarımdan sadece birinin bile olmaması da söz konusu bilgisayarın güvenliksiz sayılmasını gerektirir. Kötü niyetli kişiler, bu bilgisayarları internet üzerinden yaptıkları basit taramalarla keşfedip, bulaştırdıkları zararlı yazılımlarla kontrolü ele geçirebiliyorlar. Bu zararlılarla bilgisayarınızdan farklı kişilere/kurumlara saldırabiliyor, bilgisayarınızın üzerinde kamera, mikrofon vb. varsa ortam izlemesi ya da dinlemesi yapabiliyorlar. Ya da en basitinden, bilgisayarınızdan

girdiğiniz Facebook, Messenger, Instagram vb. hesaplarınızın kullanıcı adı ve şifrelerini çalabiliyorlar. Dolayısıyla antivirüs'e neden para ödeyeyim, gizli verim yok ki diye düşünürken, bir sabah uyanıp bilgisayarınızdan bir bankaya saldırıldığını öğrenebilir ya da bir kişiye hakaret içeren bir yazı yazıldığı için gözaltına alınabilirsiniz. Ya da referanslar kısmında belirttiğim örnek olaylardaki gibi (Radikal'in haberi), gizlice kamera görüntüsü çeken bir dolandırıcının veya sapığın şantajına maruz kalabilirsiniz. Dolayısıyla siz siz olun, lisanslı programlar kullanın ve antivirüs programınızı yükleyip güncel tutun!

Ayrıca, e-postalar olsun, Facebook/Instagram gibi platformlar olsun, bilmediğiniz kişi ve kurumlardan gelen hiçbir e-posta, ilan, kopyala yapıştır gibi şeyleri açmayın, kopyalamayın, tıklamayın.

Sosyal medya hesaplarınıza sadece güvenilir cihazlarınız (orijinal işletim sistemine sahip, antivirüs ve güvenlik güncellemeleri yüklü cihazlar) üzerinden login olun ve güvenlik-gizlilik ayarlarınızı yapın. Bilinmeyen cihazlardan giriş yapıldığında uyarı veren giriş uyarılarınızı aktif hale getirmeyi ve örneğin Facebook ile giriş yap seçeneği kullandığınız uygulamalar ile paylaştığınız bilgileri kontrol etmeyi unutmayın.

FACEBOOK DOLANDIRICILIKLARI

Ele geçirilen Facebook hesapları çoğunlukla kişinin arkadaşlarının ya da ailesinin dolandırılması için kullanılıyor. Örneğin dolandırıcı, kişinin hesabından arkadaşlarına attığı mesajlarda, çok zor durumda olduğunu bildiriyor ve kendisine acilen para gönderip gönderemeyeceklerini soruyor. Gönderilen paralar genellikle önceden dolandırıcılar tarafından ele geçirilmiş başka kurbanların hesapları olduğundan, maalesef giden paralar çoğunlukla geri alınamıyor. Diğer bir örnekte de dolandırıcı, kişinin çalıştığı şirketin bir kampanya yaptığını ve kimlik bilgilerini ve/veya kredi kartı bilgilerini gönderen arkadaşlarını bu kampanyadan yararlandırabileceğini iletiyor. Bilgilerini gönderen arkadaşların yine yandığını söylememe gerek yok sanırım. Ama bazı arkadaşlar daha dikkatli oluyor, kişinin gerçekten o olduğunu anlamak için sorular soruyorlar: Eşinin adı, çocuk sayısı, kedinin adı gibi. Ah keşke bu bilgileri de sosyal medyada paylaşmasaydık; ama maalesef paylaşmak istiyoruz ve dolandırıcılar paylaştığımız bu bilgileri çalışıyorlar. Hatta çalıştıkları bilgileri kopyalayarak bizim adımıza ikinci hesaplar açıp oradan da arkadaşlarımızı dolandırabiliyorlar.

Facebook üzerinden yapılan dolandırıcılıklar saymakla bitmiyor, kişinin hoşlandığı şeyleri

belirleyip, yalnız olduğunu saptadıkları kişilerle arkadaşlık kuran, evlenen ve parasını alanlar, evini soyup kaçanlar gibi.

INSTAGRAM DOLANDIRICILIKLARI

Instagram'da da Facebook'takine benzer dolandırıcılıklara rastlanılmaktadır ama benim en çok duyduğum, Instagram'da binlerce takipçisi olan, çok güzel yorumları bulunan hesaplardan yapılan satışlarda, ödemesi alınan ürünlerin gönderilmediği ya da gönderilen ürünle hesapta sergilenen ürünün birbirinden çok farklı olduğu. Tabii ödeme alındıktan sonra, ilgili hesaba yorum yapmanız ya da satıcının telefon numarasını aramanız engelleniyor. Bunun yarısını şimdi öde, tamamını kargoda öde gibi versiyonlar da mevcut.

Özetle, teknolojinin getirdiği kolaylıklardan yararlanırken, bir yandan da hem kendi hem de sevdiklerimizin güvenliği için risklerin farkında olmalıyız. Instagram'da tanımadığımız kişiye verdiğimiz sipariş adresi bilgisinin, Facebook ya da Foursquare'de tatildeyiz bilgisi ile eşlendiğinde çok daha büyük anlamlar taşıyabileceğinin farkında olmalıyız. Tanımadığımız kişilerin paylaşımlarımızı görmemesi için hesaplarımıza girdiğimiz cihazların güvenilir olmasını sağlamalı, hesaplarda kullanabileceğimiz güvenlik ve gizlilik önlemlerini inceleyip aktif hale getirmeliyiz.

Güvenli günler !

REFERANSLAR

» http://www.radikal.com.tr/turkiye/iste-basbakanin-bahsettigi-santaj-virusu-1177364/
» http://www.iha.com.tr/haber-facebookta-hediye-ceki-dolandiriciligi-621662/
» http://www.hurriyet.com.tr/ekonomi/instagramda-dolandiricilarin-oltasina-takilmayin-40800255

YAZAR HAKKINDA

Pelin Pehlivan bankacılık, telekomünikasyon ve enerji sektörlerinde Siber güvenlik ve IT denetimi alanlarında 19 yılı aşkın bir tecrübeye sahiptir. Etik hacker (CEH), IT denetimi (CISA), Risk Yönetimi (CRISC), Bilgi Güvenliği Yönetim Sistemi Denetimi (27001 LA) ve IT Yönetişimi (COBIT) sertifikalarına sahip olan Pehlivan, Enerjisa'da Siber Güvenlik Risk ve Uyum Grup Müdürü olarak çalışmakta, aynı zamanda da ISACA İstanbul ve TİDE yönetim kurullarında görev yapmaktadır.