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

OCAK 2017

Çevrimiçi (online) Güvenlik İpuçları

BU YAZIYI OKUMAYA BAŞLADIĞINIZA GÖRE, SİZİN DE TEMEL İHTİYAÇLARINIZDAN BİRİ İNTERNET'E BAĞLI OLMAK, YANİ İLGİLİ UYGULAMA ÜZERİNDEN ERİŞEBİLİR VE ERİŞİLEBİLİR OLMAKTIR.

Sürekli çevrimiçi olma ihtiyacı bizleri, başta mobil ve kablosuz ağlar olmak üzere, internet erişimi olanağı tanıyan çeşitli ortamları kullanmaya yöneltmektedir. Ancak tercih edebileceğimiz, internet erişimini bize sağlayanı tanımadığımız, güvenilmez aracılarla internete bağlanmak, kimlik, para ve itibar kaybetmemize neden olabilecek büyük riskleri de beraberinde getirmektedir.

Çevrimiçi olmanın risklerini nasıl yönetebiliriz? Halka açık alanlardaki kablosuz internet noktalarına bağlanırken dikkat etmemiz gerekenler nelerdir? Hangi basit yöntemlerle güvenliğimizi koruyabiliriz?

NEDEN BU RİSKLER HAYATIMIZDA?

İnternetin geliştirilmesine yönelik ilk çalışmalar, II. Dünya Savaşı'ndan sonraki savaşın atom bombalarıyla yapılacağını düşünen ABD yetkililerinin, sığınaklardan silah sistemlerini yönetme ihtiyacı nedeniyle ortaya çıkmıştır. Sadece askeri amaçlarla ve sonrasında da üniversitelerin akademik kullanımı için planlanan bu ağ, kapalı ve özel kurumlar için tasarlandığından, "güvenlik" ilk tasarım kriterleri arasında kendisine yer bulamamıştır. Üstelik bu sorun zamanla büsbütün büyümüş ve günümüzde de mücadele etmek durumunda kaldığımız önemli bir alan haline gelmiştir.

Güvenlik daha sonra yama yöntemiyle eklenmeye çalışıldığından, ek araç olarak kullanıcılara, bilgi ve davranışlarla desteklenmesi gereken ek bedeller getirmiştir. Bu bedelleri ödemeyenler ise internetin hırsızlık ve bilgi kaybı gibi olumsuz yönleriyle karşı karşıya kalmaktadır.

KABLOSUZ İLETİŞİM

"Doğada kablo yoktur" demişti bir arkadaşım yıllar önce. Kablosuz ağlar, kullanacağımız cihazı tam olarak nerede, fiziki mekânın hangi katında, hangi odasında, hatta hangi köşesinde kullanmamız konusunda temel bir kısıtlamayı bizlere dayatan kablolu iletişim ağlarına güçlü bir alternatif olarak ortaya çıkmıştır.

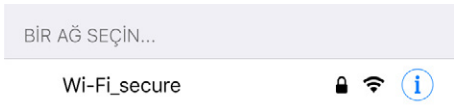
İngilizce "wireless fidelity" kelimelerinin ilk harflerinden türetilmiş olan wi-fi kelimesi ilk olarak 1999 yılının Ağustos ayında kullanılmış, günümüzde ise modern hayatın olmazsa olmaz teknolojisi haline gelmiştir. Wi-Fi'da da, gerçek hayatın en temel özelliği olan güvenlik ihtiyacına çözüm yaratma başta ne yazık ki fark edilmemiş, tercih edilmemiştir. Dolayısıyla, sonradan eklenen güvenlik özellikleri için kullanıcıların dikkat ve çaba göstermesi gerekmektedir.

GÜVENLİ KABLOSUZ İLETİŞİM İÇİN PRATİK ÖNERİLER

Günümüz dünyasında risk almadan iş yapmak mümkün değildir. Ancak ilgili risk, yaptığımız işten elde edeceğimiz potansiyel faydadan daha büyük olmamalıdır. Biraz dikkat ve çabayla çevrimiçi risk düzeyi azaltılabilir. Aşağıda belirtilen bazı hususları göz önünde bulundurarak ve önerileri değerlendirerek olası riskler için önlemler alabilir, daha bilinçli tercihlerde bulunulabilirsiniz:

- Kablosuz erişimi ne amaçla kullanacağınızı değerlendirin; güncel haberleri mi gözden geçireceksiniz (düşük risk etkisi), yoksa bankacılık, borç ödeme, e-devlet ve benzeri hassas uygulamaları kullanacağınız (yüksek risk etkisi) bir erişim mi gerçekleştireceksiniz? Riskleri göz önüne alın ve riskli olabilecek kablosuz hizmeti kullanıp kullanmayacağınıza ona göre karar verin.
- Otel, okul, kafe işletmesi gibi kablosuz ağ hizmeti sunan tarafların büyük bir kısmı kendi içlerinde temel güvenlik önlemlerini almıyorlar. Bu nedenle bu ağlar üzerinden yaptığınız işlemler, saldırganların hedefi olabilir. Yüksek risk etkili bir işlem yapacaksanız, kendi eviniz ve iş yeriniz gibi güvenilir ağları ya da mobil operatörlerin internet bağlantılarını tercih edin.

» İletişiminizin güvenliği için HTTPS, WPA2, SSL, VPN ve benzeri yöntemlerin kullanılması gerekir. Şifreleme araçlarını yerinde ve doğru bir şekilde kullanmıyorsanız, iletişiminiz kontrolünüz dışında izlenebilir. Sizin yönettiğiniz kablosuz bağlantıların, güvenli protokol (WPA2) üzerinden sağlandığını, gerek modem kontrol ekranındaki seçenek ile gerekse de mobil cihazınızda kablosuz ağın yanındaki kilit resminden teyit edin.

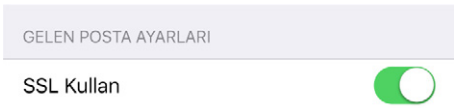


» Tarayıcılarda güvenli bağlantıyı (HTTPS) kullanın. Kritik uygulamalarda bağlanılan adresin doğruluğunu, adres satırındaki kilit işareti ve https://ifadesinin üzerine tıklayarak açılan ekranda kontrol edin.

» **Hata mesajlarına dikkat:** İnternet erişiminiz sırasında karşınıza çıkabilecek hata mesajlarında, <tamam> ya da <<sürdür> tuşuna basmadan önce, tam olarak neyi onayladığınızı okuyun.

» Yeni bir ağa bağlanmak için talep edilen kişisel bilgileri vermeden düşünün. Cep telefon numaranız veya kaldığınız oda bilgisi dışında kişisel bilgilerinizi talep eden kablosuz ağlara bağlanmayın.

» Mobil cihazınız üzerindeki, üreticisi tarafından önerilen güvenlik önlemlerini gerçekleştirin. Uzmanlarca kullanılması önerilen kişisel firewall ve anti-virüs benzeri uygulamaları kurun ve kullanın.



» Kullanmadığınız zaman mobil cihazınızdaki kablosuz ağı kapatın. Böylece hem pil ömrü uzar, hem de kablosuz ağ üzerinden yapılabilecek saldırılara karşı kendinizi korumuş olursunuz.

Hayatımızda bu denli önemli bir yer tutan internete sürekli bağlı olma ihtiyacının hem özel hem de iş hayatımız için vazgeçilmez hale geldiği söylenebilir. Bu nedenle degerekli önlemlerin alınması artık kuşkusuz üzerimize düşen en temel görevdir. Günümüzde, güvenlikle ilgili konuların öncelikle farkında olmamız, dijital dünyadaki varlıklarımızı bilmemiz, bu varlıklara yönelik olası riskleri değerlendirmemiz ve gerekli önlemleri almamız en önemli sorumluluğumuzdur.

YAZAR HAKKINDA

Tevfik Kolabaş, İTÜ Kontrol ve Bilgisayar Mühendisliği Bölümü mezunudur. Aynı üniversitede yüksek lisans derecesini almıştır. Gerçek zamanlı sistemler ve altyapılar üzerinde deneyime sahip olan Tevfik Kolabaş, ISACA Istanbul Chapter kuruluşunda aktif rol oynamış, CISSP sınavlarının yurdumuzda gerçekleşmesi sürecinde faal görev almıştır.