eGüvenlik Veli Bilgilendirme Formu

10 Maddede Güvenli İnternet Kullanımı

Hayatın neredeyse her alanında evimizde, cebimizde, kafelerde, restoranlarda, AVM'lerde ve aklınıza gelebilecek her türlü ortamda interneti özgürce kullanabiliyoruz. Bu denli büyüyen ve gün geçtikçe gelişmeyi sürdüren internetin gerek sosyal gerekse iş hayatındaki olumlu katkıları yadsınamaz ancak kimi zaman da pek çok olumsuz durumla da bizi yüz yüze bırakabiliyor. İşte bu noktada olumsuz durumları yaşamamak ya da en azından minimuma indirmek adına birtakım önlemler almak gerekiyor. Peki, güvenli internet kullanımı için yapılması gerekenler neler? Gelin bir gözden geçirelim.

1. Kişisel Bilgileri Profesyonel ve Sınırlı Tutun Potansiyel işveren veya müşterilerin kişisel ilişki durumunuzu veya ev adresinizi bilmesine gerek yok. Uzmanlık alanınızı, profesyonel geçmişinizi ve sizinle nasıl iletişim kuracaklarını belirtmiş olmanız yeterlidir. Şahsi bilgilerinizi tanımadığınız milyonlarca yabancı kişiye kendi ellerinizle teslim etmeyin.

2. Gizlilik Ayarlarınızı Açık Tutun Pazarlamacılar sizin hakkınızda her şeyi bilmek isterler aynı zamanda hackerlar da ister tabii. Her ikisi de internet taramalarınızdan ve sosyal medya kullanımınızdan birçok şey öğrenebilir. Bunun önlemini alabilmeniz için hem web tarayıcıların hem de mobil işletim sistemlerin gizliliğinizi çevrim içi korumak için çeşitli ayarlar bulunmaktadır. Ayrıca Facebook, Instagram ve Twitter gibi büyük sosyal medya uygulamalarının da gizlilik artırıcı ayarları mevcut. Bu ayarlar içerisinden aradıklarınıza erişebilmeniz bazen çok zor olabilir. Çünkü şirketler kişisel bilgilerinizi pazarlayıp maddi gelir elde etmek için kullanıyorlar. Dolayısıyla bu bilgileri gizli tutmakta ne kadar zorlanırsanız bu durum onların işlerine gelecektir. Burada sizin yapmanız gereken tüm bu güvenlik ayarlarını detaylı bir şekilde gözden geçirip önemli olanlar başta olmak üzere tüm güvenlik ayarlarınızın açık olduğundan emin olmalısınız.

3. Gördüğünüz Her Linke Tıklamayın Tehlikeli bir semtte yürümeyi tercih etmezsiniz değil mi? O zaman tehlikeli web sitelerinde de dolaşmamalısınız. Siber suçlular, bu tarz tehlikeli gibi gözükmeyen ancak içerisinde birçok tuzak barındıran sahte içerikleri birer yem olarak kullanırlar. Siber suçlular birçok insanın arama yaptıkları esnada buldukları kaynaklar şüpheli dahi olsa merak duygularına yenik düşeceklerini ve içeriklerin cazibelerine kapılıp gardlarını indireceklerini biliyorlar. Bu tarz dikkatsiz tıklamalar sonucunda kişisel verilerinizin açığa çıkabileceği gibi elektronik cihazlarınıza malware diye tabir edilen kötü amaçlı yazılımların yüklenmesine de sebebiyet verebilir. Dolayısıyla içinizdeki dürtülere direnerek o şüpheli gördüğünüz içeriklerdeki linklere tıklayıp hackerlara sizi hacklemeleri için fırsat tanımamalısınız.

4. İnternet Bağlantınızın Güvenli Olduğundan Emin Olun Halka açık bir yerde, örneğin herkese açık bir Wi-Fi bağlantısı kullanarak çevrim içi olduğunuzda, artık cihazınızın güvenliğinin üzerinde doğrudan kontrolünüz olmadığını bilmelisiniz. Bu sebepten siber

güvenlik uzmanları birliği dış dünya ile bağlantı kurduğunuz halka açık özel ağlar ile ilgili oldukça endişeliler. Onların tavsiyesine göre eğer banka hesap numaranız gibi önemli bilgileri girecekseniz önce cihazınızın bağlandığı ağın güvenli olduğundan emin olmalısınız. Eğer güvenlik ile ilgili herhangi bir şüpheniz varsa, güvenli bir Wi-Fi ağına bağlanana kadar beklemelisiniz.

5. Ne İndirdiğinize Dikkat Edin Siber suçluların en önemli amacı, kişisel bilgilerinizi çalmaya çalışan veya bilgisayarınızı kendi kötü çıkarları için kullanmaya çalışan kötü amaçlı yazılımları indirmenizi sağlamaktır. Bu kötü amaçlı yazılımlar popüler bir oyunun içerisine saklanabileceği gibi, trafik durumunu veya hava durumunu kontrol eden uygulamanın içerisinde de saklı bulunabilmektedir. Dolayısıyla şüpheli gördüğünüz veya güvenmediğiniz sitelere ait uygulamaları indirmemelisiniz.

6. Güçlü Şifreleri Seçin Şifreler, tüm internet güvenliği yapısında en büyük zayıf noktalardan biridir. Günümüzde parolalarla ilgili esas problem, insanların siber hırsızların tahmin etmeleri kolay olan şifreler kullanmalarıdır. İnsanlar hatırlanması kolay olan şifreleri seçme eğiliminde olduklarından dolayı şifrelerini basit seçmektedirler. Eğer elektronik aygıtlarınızın ve internet üzerinde bulunan tüm hesaplarınızın güvenliklerini arttırmak istiyorsanız siber suçluların tahmin etmesi zor olan güçlü şifreleri seçmeye özen göstermelisiniz. Güçlü bir parola belirleyebilmek için, benzersiz kelime grupları oluşturmalı ve en az 15 karakter uzunluğunda, harfleri, sayıları ve özel karakterleri barındıran şifreler kullanmalısınız.

7. Güvenli Sitelerden Satın Alım Yapın Çevrim içi bir ürün satın aldığınızda, kredi kartı veya banka hesabı bilgilerini kullanmanız gerekmektedir. Dolayısıyla bu bilgileri güvenli, şifreli bağlantılar sağlayan sitelere girmeniz hayati önem taşımaktadır. Ürün satın almadan önce kart bilgilerini gireceğiniz web sitelerinin https: ile başladığından emin olmalısınız. Eğer yalnızca http: ile başlıyorsa o siteden kesinlikle alışveriş yapmamalısınız. Burada sonda bulunan “S” ifadesi secure yani güvenli anlamına gelmektedir.

8. Ne Yazdığınıza Dikkat Edin İnternette bir silme anahtarı yoktur yani sizin internet üzerinde paylaştığınız tüm yorumlar, resimler ve içerikler silseniz dahi internet üzerinde sonsuza dek kalabilirler. Çevrim içi gönderdiğiniz herhangi bir yorum veya resim Twitter’dan kaldırılmış olsa dahi, başkalarının sildiğiniz içeriği kendi bilgisayarına kopyalamadığından %100 emin olamazsınız. Dolayısıyla içerik paylaşırken ailenizin, potansiyel işvereninizin ve geri kalan çevrenizin görmesini istemeyeceğiniz şeyler paylaşmamaya özen gösterin.

9. Kiminle Tanıştığınıza Dikkat Edin Çevrim içi olarak tanıştığınız kişiler, her zaman iddia ettikleri kişiler olmayabilir. Hatta gerçek kişiler bile olmayabilirler. As InfoWorld’ün raporlarına göre, sahte sosyal medya profilleri sıradan sosyal medya kullanıcıların kullandığı bir yöntem olduğu kadar hackerlar için de insanların hesaplarını çalmak amacıyla kullandıkları

popüler bir yoldur. O yüzden çevrimiçi sosyal yaşamınızda, kişisel sosyal yaşamınızda olduğunuz kadar dikkatli ve mantıklı olmanızda fayda vardır.

10. Virüs Koruma Programınızı Güncel Tutun İnternet güvenlik yazılımlarınız sizi her tehdide karşı koruyamayacaktır, ancak bu yazılımları güncel tuttuğunuz müddetçe sizi birçok malware virüslerinden koruyacaklardır. Dolayısıyla, işletim sisteminizin ve kullandığınız başta güvenlik yazılımlarınız olmak üzere tüm uygulamaların güncellemelerini aksatmadan düzenli bir şekilde yapmalısınız. Eğer yukarıda bahsettiğimiz bu 10 temel internet güvenliği kuralını aklınızda bulundurup dikkatlice internette dolaşırsanız kötü sürprizlerin çoğunu önleyeceğinizden emin olabilir