

# 10 MADDEDE

## GÜVENLİ İNTERNET KULLANIMI

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 bir çok şey öğrenebilir. Bunun önlemini alabilmeniz için hem web tarayıcıların hem de mobil işletim sistemlerin gizliliğinizi çevrimiçi 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 bir çok tuzak barındıran sahte içerikleri birer yem olarak kullanırlar. Siber suçlular bir çok 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 yazılımlarını 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 çevrimiçi olduğunuzda, artık cihazınızın güvenliğinin üzerinde doğrudan kontrolünüz olmadığını bilmelisiniz. Bu sebepten dolayı siber güvenlik uzmanları

birliđi dıř dŸnya ile bađlantı kurduđunuz halka ađık Ÿzel ađlar ile ilgili oldukça endiřeliler. Onların tavsiyesine gŸre eđer banka hesap numaranız gibi Ÿnemli bilgileri girecekseniz Ÿnce cihazınızın bađlandıđı ađın gŸvenli olduđundan emin olmalısınız. Eđer gŸvenlik ile ilgili herhangi bir řŸpheniz varsa, gŸvenli bir Wi-Fi ađına bađlanana kadar beklemelisiniz.

## **5. Ne İndirdiđinize Dikkat Edin**

Siber suđluların en Ÿnemli amacı, kiřisel bilgilerinizi çalmaya çalıřan veya bilgisayarınızı kendi kŸtŸ çıkarları iin kullanmaya çalıřan kŸtŸ amalı yazılımları indirmenizi sađlamaktır. Bu kŸtŸ amalı yazılımlar popŸler bir oyunun ierisine saklanabileceđi gibi, trafik durumunu veya hava durumunu kontrol eden uygulamanın ierisinde de saklı bulunabilmektedir. Dolayısıyla řŸpheli gŸrdŸđŸnŸz veya gŸvenmediđiniz sitelere ait uygulamaları indirmemelisiniz.

## **6. GŸçlŸ řifreleri Sein**

řifreler, tŸm internet gŸvenliđi yapısında en bŸyŸk zayıf noktalardan biridir. GŸnŸmŸzde parolalarla ilgili esas problem, insanların siber hırsızların tahmin etmeleri kolay olan řifreler kullanmalarıdır. İnsanlar hatırlanması kolay olan řifreleri seme eđiliminde olduklarından dolayı řifrelerini basit semektedirler. Eđer elektronik aygıtlarınızın ve internet Ÿzerinde bulunan tŸm hesaplarınızın gŸvenliklerini artırmak istiyorsanız siber suđluların tahmin etmesi zor olan gŸçlŸ řifreleri semeyeŸzen gŸstermelisiniz. GŸçlŸ bir parola belirleyebilmek iin, benzersiz kelime grupları oluřturmalı ve en az 15 karakter uzunluđunda, harfleri, sayıları ve Ÿzel karakterleri barındıran řifreler kullanmalısınız.

## **7. GŸvenli Sitelerden Satın Alım Yapın**

evrimii bir ŸrŸn satın aldıđınızda, kredi kartı veya banka hesabı bilgilerini kullanmanız gerekmektedir. Dolayısıyla bu bilgileri gŸvenli, řifreli bađlantılar sađlayan sitelere girmeniz hayati Ÿnem tařımaktadır. ŸrŸn satın almadan Ÿnce kart bilgilerinizi gireceđiniz web sitelerinin https: ile bařladıđından emin olmalısınız. Eđer yalnızca http: ile bařlıyorsa o siteden kesinlikle alıřveriř yapmamalısınız. Burada sonda bulunan "S" ifadesi secure yani gŸvenli anlamına gelmektedir.

## **8. Ne Yazdıđınıza Dikkat Edin**

İnternette bir silme anahtarı yoktur yani sizin internet Ÿzerinde paylařtıđınız tŸm yorumlar, resimler ve ierikler silseniz dahi internet Ÿzerinde sonsuza dek kalabilirler. evrimii gŸnderdiđiniz herhangi bir yorum veya resim Twitter'dan kaldırılmıř olsa dahi, bařkalarının sildiđiniz ieriđi kendi bilgisayarına kopyalamadıđından %100 emin olamazsınız. Dolayısıyla ierik paylařırken ailenizin, potansiyel iřvereninizin ve geri kalan evrenizin gŸrmesini istemeyeceđinizřeyler paylařmamaya Ÿzen gŸsterin.

## **9. Kiminle Tanıřtıđınıza Dikkat Edin**

evrimii olarak tanıřtıđınız kiřiler, her zaman iddia ettikleri kiřiler olmayabilir. Hatta gerek kiřiler bile olmayabilirler. As InfoWorld'Ÿn raporlarına gŸre, sahte sosyal medya profilleri sıradan sosyal medya kullanıcıların kullandıđı bir yŸntem olduđu kadar hackerlar iin de insanların hesaplarını çalmak amacıyla kullandıkları popŸler bir yoldur. O yŸzden evrimii sosyal yařamınızda, kiřisel sosyal yařamınızda olduđunuz 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 bir çok malware virüslerinden koruyacaklardır. Dolayısıyla, işletim sisteminizin ve kullandığınız başta güvenlik yazılımlarınız olmak üzere tüm uygulamaların güncellemelerini aksatmadan düzenli bir şekilde yapmalısınız.

---