STOP | THINK | CONNECT™

Güvenli bir Online Alışveriş için Öneriler

Mobil cihazlar - akıllı telefonlar, dizüstü bilgisayarlar ve tabletler gittiğiniz her yerde, her zaman elinizin altında olup, iş, seyahat, eğlence ya da farklı amaçlar için kullanılmaktadır. Bu cihazlar çevrenizdeki dünyaya kolayca bağlanmanızı sağlar. Ancak içerisinde kişiler, fotoğraflar, videolar, konumlar, sağlık ve mali veriler gibi siz veya yakınlarınız hakkında bir çok bilgiyi barındırmaktadır. Bu bağlamda taşınabilir cihazlarınızı güvenli bir şekilde kullanmak çok önem arz etmektedir. İlk önce, güvenlik tedbirleri alarak, çevrimiçi gerçekleştirilen eylemlerin sonuçlarını düşünmek gerekmektedir. Daha sonra gönül rahatlığıyla teknolojinin getirdiği kolaylığın keyfi çıkarılabilir.

KİŞİSEL BİLGİLERİNİZ PARA GİBİDİR. BUNLARA DEĞER VERİN VE KORUYUN

Cihazlarınızı Güvenli Hale Getirin: Cihazlarınızı kilitlerken güçlü parolalar belirleyin veya cihazınızın dokunmatik kimlik özelliklerinden faydalanın. Bu şekilde cihazınız hem meraklı gözlerden uzak kalır hem de kayıp veya çalıntı gibi durumlarında bilgileriniz korunmuş olur.

Uygulamaları İndirmeden Önce bir daha düşünün
Beğendiğiniz oyunlar, kartvizit listeniz, alışverişleriniz ve konumunuz gibi sizi ilgilendiren bilgiler para gibi değerlidir. Uygulamalar yoluyla toplanan bu bilgilerin kim tarafından ve nasıl elde edildiği hakkında bir kez daha düşünün.

KULLANILMIYORSA, WIFI VE BLUETOOTH DEVRE DIŞI BIRAKILMALIDIR

Bazı mağazalar ve çeşitli yerler, kendi aralığında bağlı olan cihazları Wi-Fi veya Bluetooth ile izlemektedir. Kullanılmıyorsa, WiFi ve Bluetooth devre dışı bırakılmalıdır.

WiFi Noktaları Hakkında Bilinçli Olun
Halka açık kablosuz ağlar ve mobil veri paylaşım noktaları güvenli değildir. Bunlara bağlı olan herhangi biri mobil cihazınızda potansiyel olarak ne yaptığınızı görebilirir. Bu bağlamda halka açık WiFi ağlarında yapmak istediklerinizi sınırlayınız ve özellikle e-mail ve mali hizmet gibi önemli hesaplara giriş yapmaktan kaçınınız. Eğer gerekirse bir sanal özel ağ (VPN) veya kişisel / mobil hotspot kullanmalısınız.

Makineniz Temiz Kalmalı
Mobil Cihazlarınızı ve uygulamalarınızı Güncel Tutun: Mobil cihazlarınız da PC'leriniz ya da dizüstü bilgisayarlarınız kadar savunmasızdır.

En son çıkan ve en güncel güvenlik yazılımları, web tarayıcıları ve işletim sistemleri, virüsler, kötü amaçlı yazılımlar ve diğer çevrimiçi tehditlere karşı en iyi savunmadır. Bu bağlamda yazılımlar ve uygulamalar güncel olmalı.

İşiniz Bittiğinde Silin: Birçoğumuz uygulamaları bir tatil planlama gibi belirli amaçlar için indiririz ve daha sonra bu uygulamalara ihtiyacımız olmaz. Ayrıca önceden gerekli olan ve daha sonra işimize yaramayan bir çok uygulama olabilir. Bu yüzden kullanmadığınız tüm uygulamaları silmek iyi bir güvenlik tedbiridir.