**DİJİTAL GÜVENLİK**

Dijital dünyada dijital güvenliği sağlamak için hem dijital hem de fiziksel önlemler almak gerekebilir. Dijital güvenliğin sağlanamaması sonucunda kişisel veriler çalınabilir, maddi ve/veya manevi zararlara sebep olan sonuçlara maruz kalınabilir.

Günde yaklaşık olarak yedi saatini çevrimiçi geçiren bir ülke olarak dijital dünyanın tehlikelerini bilmek ve bunlara karşı önlem almak büyük önem taşımaktadır. [Dijital güvenlik için VPN kullanımı](https://www.expressvpn.com/tr/what-is-vpn), antivirüs kullanımı, kişisel veri ve bilgilerin nasıl korunması gerektiği, aktif ve pasif dijital ayak izleri üzerinde durulması gereken konulardır.

**Dijital Güvenlik İçin VPN**

Dijital güvenlik için VPN kullanımı hem şirketler hem de bireyler tarafından tercih edilen bir yöntemdir. Virtual Private Network yani Sanal Özel Ağ (VPN) teknolojisi ortak kullanılan internet üzerinde tünel protokolleri ile birlikte sanal özel bir ağ oluşturur. Bu sanal özel ağ üzerinden akan veriler internet servis sağlayıcısı tarafından dahi görülemez.

Dijital güvenlik adına internet trafiğinin herhangi bir üçüncü partiden gizlenmesi kişisel bir özgürlüktür. VPN kullanımı aynı zamanda erişilemeyen web sitelere de kullanıcının erişmesini sağlayarak ona internet özgürlüğü sağlar. VPN kullanmanın güvenlik sağladığı asıl kısım kullandığı şifreleme algoritmaları ile bağlantılıdır. Başkaları tarafından görülmeyen ağ üzerinden akan veri paketleri çeşitli şifreleme algoritmaları ile şifrelenerek varış noktasına kadar şifreli bir şekilde seyahat eder.

**Dijital Güvenlik İçin Güvenli Web Siteler**

Dijital güvenlik için her zaman SSL sertifikasına sahip web siteler üzerinden alışveriş yapılmalıdır ve SSL sertifikasına sahip olmayan web siteler üzerinden herhangi bir kişisel veri ve bilgi paylaşımından kaçınılmalıdır. SSL –[Güvenli Soket Katmanı](https://www.internethaber.com/internetten-alisverise-dikkat-387729h.htm)– sertifikasına sahip web siteler o web siteyi ziyaret eden kişi ve o web sitenin sunucusu arasında seyahat eden verileri şifreleyerek güvenli bir ortam oluşturur.

SSL sertifikasına sahip olan web sitelerin URL kısmında bir kilit işareti ve ‘’Güvenli’’ ibaresi çıkar. Bu web sitelerin URL’si HTTPS ile başlar. SSL sertifikasına sahip olmayan web sitelerin URL kısmında ise ‘’Güvenli Değil’’ ibaresi çıkar ve bu web sitelerin URL’si HTTP ile başlar.

**Dijital Güvenlik İçin E-postalara Dikkat**

Dijital güvenlik için elektronik posta kullanımında dikkatli olunmalıdır. Siber saldırganlar tarafından kimlik, kredi kartı ve benzeri gibi bilgileri elde etmek için kullanılan yöntemlerden biri de [phishing](https://www.sozcu.com.tr/2018/ekonomi/amman-oltaya-gelmeyin-oltalama-nedir-phishing-nedir-2169577/)(oltalama) yöntemidir. E-posta üzerinden toplu olarak birçok bireye yanıltıcı bir e-posta gönderilir. Bu e-postanın içeriği resmi bir kurumu ya da bilinen bir kişiyi taklit eder.

Hesapta şüpheli aktivite durumu, kartınızdan para çekildi, şifreniz değiştirildi ve benzeri gibi elektronik posta alıcısını paniğe iten mesaj içerikleriyle bireylerin bir linke tıklamaları ya da dosya ekini indirmeleri istenir. Siber saldırganların yönlendirdiği link yine taklit edilen bir web site olur ve bireylerden bilgilerini hesaplarını kurtarmaları için girmeleri istenir. Bu şekilde siber saldırganlar hassas kişisel bilgileri ele geçirir. Elektronik postadaki dosya ekleri ise genelde kötü amaçlı yazılım içerir. Bu kötü amaçlı yazılımlar fidye yazılımları, casus yazılımları, truva atları, solucanlar, virüsler ve daha birçoğu olabilir.

**Dijital Güvenlik İçin Antivirüs**

Dijital güvenliği sağlamak için antivirüs programları kullanılmalıdır. Antivirüs programları ister akıllı telefon ister bilgisayar olsun dijital cihazları kötü amaçlı yazılımlardan korumaya yardımcı olur. Ücretsiz antivirüs programları kullanılmamalı ve lisanslı antivirüs programları tercih edilmelidir.

Kaynak: <https://teketekhaber.com/dijital-guvenlik-nasil-saglanir-56153h.html>