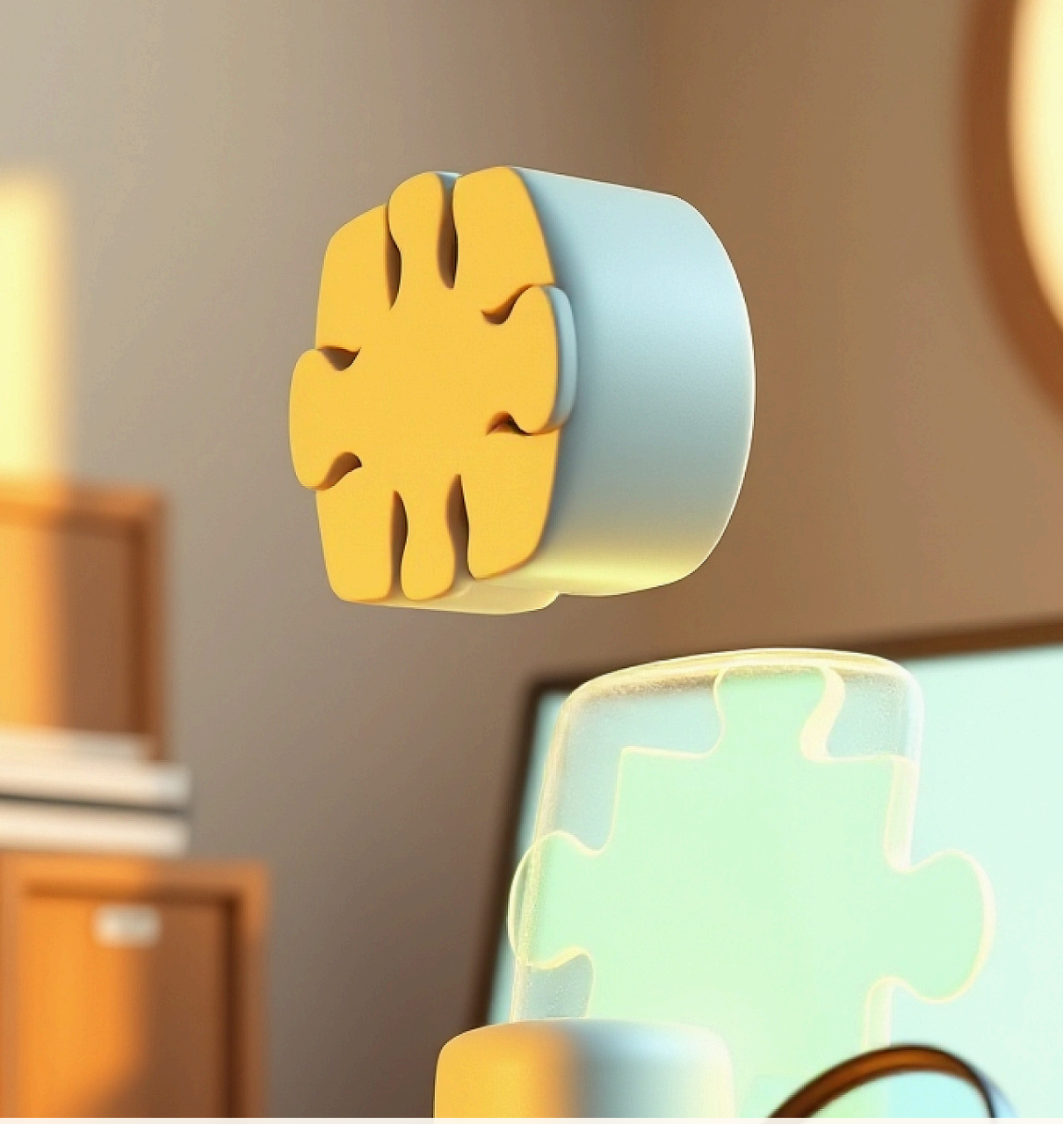
HTTPS neden kullanılır?



www.yzokul.com.tr

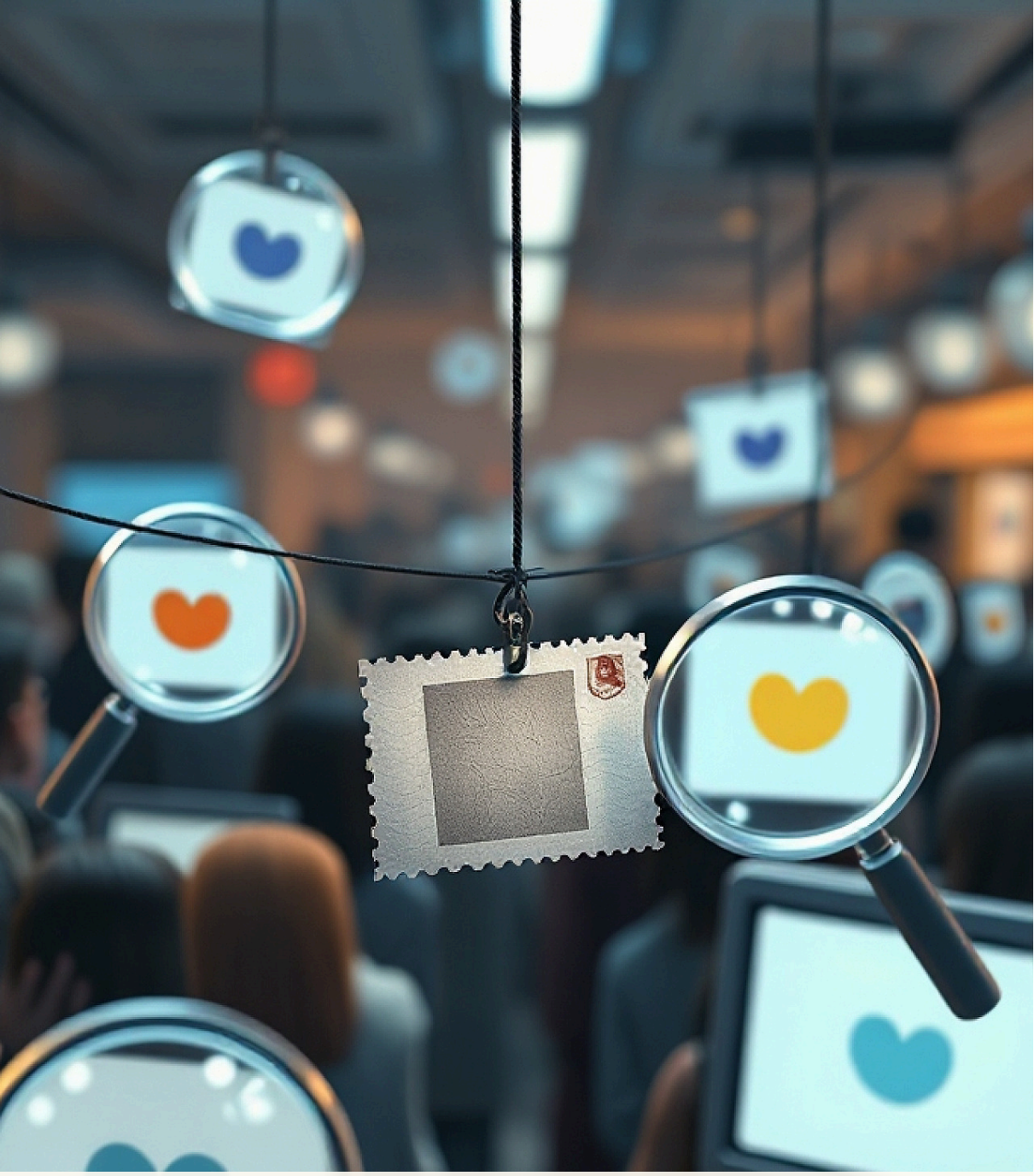
HTTPS neden kullanılır?



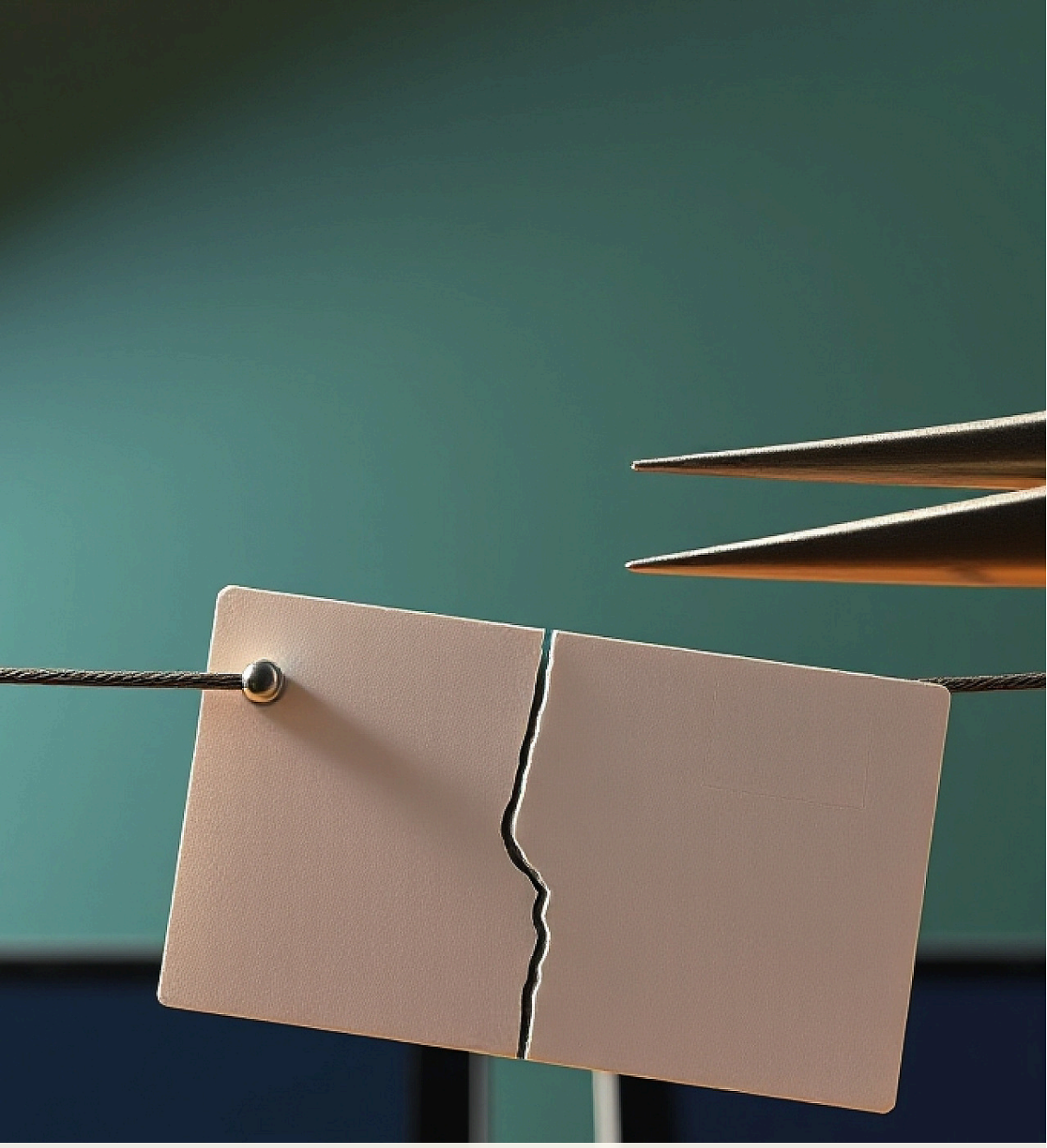
HTTPS neden kullanılır? Kısa cevap, HTTPS'in şifreli ve kurcalanmaya karşı denetlenen bir bağlantı üzerinden gönderilen HTTP olduğudur. HTTP, tarayıcının bir web sitesiyle konuşmak için kullandığı kurallar bütünüdür. Şifreleme, trafiği başkaları kolayca okuyamayacak şekilde karıştırır. Kurcalama denetimi, aktarım sırasındaki değişikliklerin fark edilmesi anlamına gelir. Bu cevabın her parçası sonraki sayfalarda ayrıntılı olarak açıklanır.



Bir web sitesini açtığında tarayıcın ile sitenin sunucusu istek ve yanıt alışverişinde bulunur. Bu mesajlar HTTP adı verilen bir kurallar bütününe uyar; HTTP, HyperText Transfer Protocol'ün kısaltmasıdır. Düz HTTP'de bu istekler ve yanıtlar sıradan, okunabilir metin olarak yol alır. HTTPS'in koruma altına alacağı şey tam olarak bu düz alışveriştir. Önce HTTP'yi anlamak, HTTPS'in nedenini netleştirir.



Postayla kartpostal gönderdiğini düşün: onu eline alan herkes arkasındaki mesajı okuyabilir. Düz HTTP trafiği de ortak bir ağda, örneğin halka açık Wi-Fi'de aynı şekilde çalışır. Aynı ağdaki biri trafiğe bakıp ne gönderildiğini okuyabilir. Bu okunabilirlik, HTTPS'in çözmek için tasarlandığı ilk sorundur. Mesele her şeyi saklamak değil, içeriği korumaktır.



Düz HTTP'nin ikinci sorunu, trafiğin geçerken değiştirilebilmesidir. Ağdaki bir aracı kişi, aktarım sırasındaki verileri sessizce değiştirebilir. Alıcı o zaman fark etmeden farklı bilgiler alır. Buna ortadaki adam saldırısı denir ve formları, indirmeleri veya sayfa içeriğini etkileyebilir. HTTPS bu riski, sessiz değişiklikleri fark edilebilir hale getirerek ele alır.



HTTPS aynı HTTP konuşmasıdır, ancak şifreli bir tünelin içinde taşınır. Tarayıcı hâlâ sayfa ister, sunucu hâlâ yanıtlar; web aynı şekilde çalışır. Yalnızca sarmalama değişir: trafik yol alırken korunur. Bunu kartpostalı kapalı bir zarfa koymak gibi düşün. Adres görünür, ama mesaj görünmez.



Şifreleme, okunabilir trafiği dışarıdakilerin kolayca anlayamayacağı karıştırılmış veriye dönüştürür. Her iki uç, yani tarayıcı ve sunucu, onu tekrar düz metne çevirmek için gereken anahtarlara sahiptir. Ağı izleyen herkes yalnızca karıştırılmış baytlar görür, içeriği değil. Bu, parolalar, mesajlar ve form girdileri gibi şeyleri korur. Şifreleme, HTTPS'in eklediği ilk korumadır.



Şifreli bağlantı ayrıca verinin değişmeden ulaşıp ulaşmadığını denetler. Bu özelliğe bütünlük koruması denir. Biri aktarım sırasında veriyi değiştirirse, değişiklik sessizce kabul edilmek yerine fark edilir. Alıcı, kurcalanmış veriye güvenmek yerine onu reddedebilir. Bütünlük koruması, HTTPS'in eklediği ikinci korumadır ve şifrelemeyle birlikte çalışır.



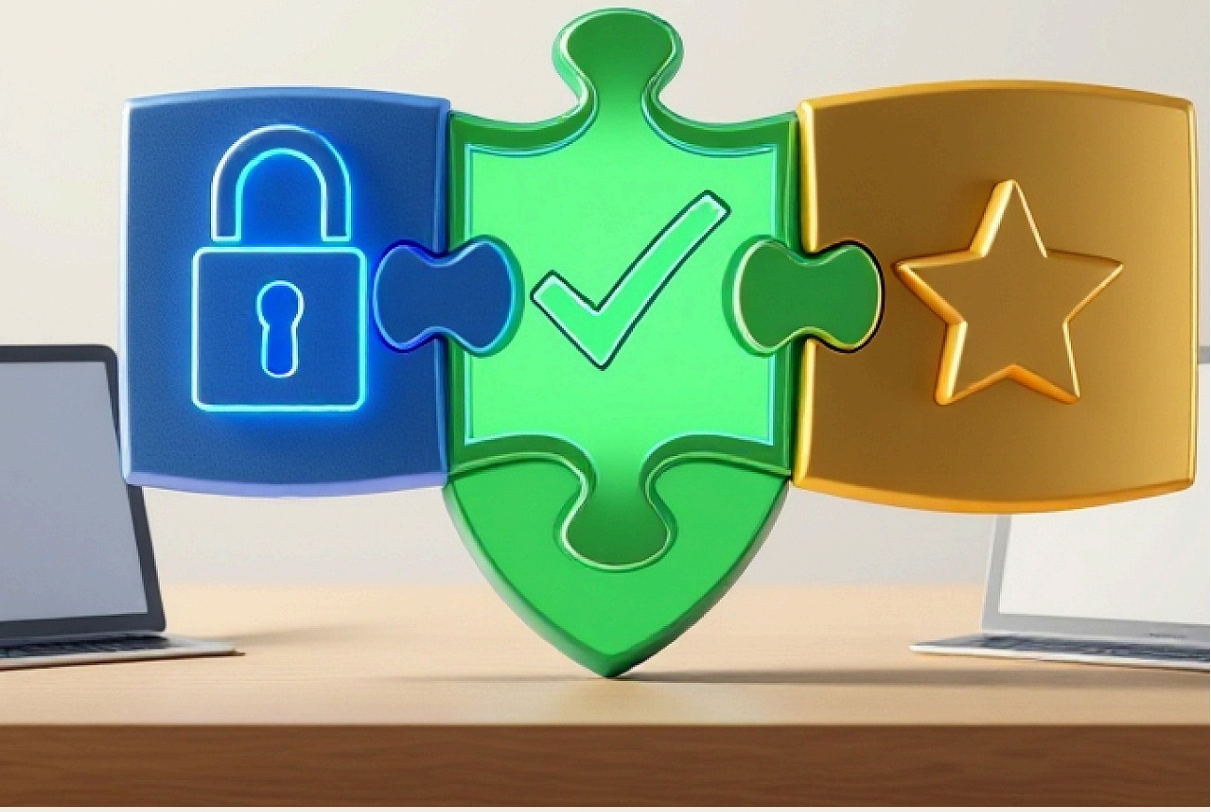
Bir sunucu, hizmet için kimlik kartı gibi işlev gören bir sertifika sunar. Tarayıcı, bağlantıya güvenmeden önce bu sertifikayı denetler. Sertifika, gerçekte hangi hizmete bağlı olduğunu doğrulamaya yardımcı olur. Sitenin içeriğini yargılamaz; yalnızca kimliği destekler. Bu kimlik denetimi, HTTPS'in eklediği üçüncü korumadır.



Güvenilir sertifika otoriteleri sertifikaları imzalar. Bunlar, kimlikleri doğrulayıp imzalı sertifika vermekle görevli kuruluşlardır. Tarayıcın güvendiği otoritelerin bir listesini taşır. Geçerli bir imza, sertifikayı denetlenmiş bir kimliğe bağlar. İmza eşleşmezse tarayıcı sertifikayı güvenilmez sayar.



Sertifika uygun çıkmadığında tarayıcı sessizce devam etmek yerine bir uyarı gösterir. Uyarı, bağlantının özel olmadığını veya sertifikanın geçersiz olduğunu söyleyebilir. Bu, kimlik denetiminin işini yapmasıdır. Ardından devam etmemeye karar verebilirsin. Uyarı bir tehlike garantisi değildir, ama dikkatli olma işaretidir.



Parçaları bir araya getirelim: HTTPS şifreli içerik, bütünlük denetimleri ve denetlenmiş bir kimliği tek bir bağlantıda sağlar. Şifreleme içeriği dışarıdakilerden gizli tutar. Bütünlük koruması sessiz değişiklikleri fark edilebilir kılar. Sertifika, ulaştığın hizmeti doğrulamaya yardımcı olur. Her parça farklı bir riski kapsar ve birlikte bağlantıyı korurlar.



HTTPS bağlantıyı korur, sitenin içeriğinin dürüstlüğünü değil. Güvenli bir tünel yine de yanıltıcı bilgi taşıyabilir. Site doğru şekilde tanımlanmış olabilir ama yine de yanlış iddialar sunabilir. Bağlantı güvenliği ile içerik güveni ayrı meselelerdir. İçerik yanlış olsa bile HTTPS işini yapar.



İki soruyu ayır: bağlantı özel ve bozulmamış mı, ve sayfadaki bilgi doğru mu? HTTPS ilk soruyu yanıtlar. İkincisini yanıtlamaz. Bir site HTTPS kullanıp yine de yanlış veya yanıltıcı içerik yayımlayabilir. Her zaman yalnızca bağlantıyı değil, bilginin kendisini de değerlendir.



Yaygın bir hata, asma kilit simgesinin sitenin güvenilir olduğu anlamına geldiğine inanmaktır. Asma kilit yalnızca bağlantının korunduğunu söyler. Sitenin sahiplerinin dürüst olduğu veya içeriğin doğru olduğu anlamına gelmez. Asma kilidi bağlantı güvenliğinin işareti olarak gör, doğruluğun işareti olarak değil. Sitenin bilgilerini ayrıca denetle.



Bir başka yaygın hata, HTTPS'in seni tamamen anonim yaptığına inanmaktır. Trafiğinin içeriğini gizler, ama başkaları belirli bir siteye bağlandığını yine de görebilir. Sayfa içeriği şifreli olsa bile alan adı görünür olabilir. HTTPS içeriği korur, bağlanma olgusunu değil. Tam anonimlik başka araçlar ve alışkanlıklar gerektirir.



Hatırlanacaklar: HTTPS sıradan web trafiğini şifreler ve bütünlük denetiminden geçirir, ayrıca hizmetin kimliğini doğrulamaya yardımcı olur. Bu korumalar, ağdaki başkaları için okumayı ve sessizce değiştirmeyi çok daha zorlaştırır. Ancak korunan bir bağlantı ile güvenilir içerik ayrı meselelerdir. HTTPS'i temel ölçüt olarak kullan ve yine de okuduğun bilgiyi değerlendir.