**BASIN BÜLTENİ**

**Seyahatteyken siber dünyada güvende kalma rehberi**

**COVID-19’un yayılma oranlarının tüm dünyada artmasına karşın ülkelerin sınırlarını turizme açmasıyla, pandemi birçok yerde daha da yüksek oranlarda geri döndü. Seyahatlerin sıklaşmasıyla birlikte siber riskler de arttı. Deloitte’un 2022 Yaz Tatili Araştırması’na göre, içinde Türkiye’nin de bulunduğu tatil ülkeleri coğrafyasında 2022 yaz dönemi ve sonbahar başlarının hareketli geçmesi bekleniyor. Bu nedenle, ülkeler arası yolculuk yapanların siber hijyene mutlaka dikkat etmesi gerekiyor.**

**Siber hijyen seyahate çıkanlar için neden önemli?**

Seyahate çıkanlar, yanlarında genellikle cihazlarını taşıyor ve bu cihazlar uç noktalar olarak biliniyor. Uç noktaların doğası ise otellerde, kurumsal ağlarda, halka açık Wi-Fi’larda veya konferanslarda farklı ağlara bağlanmayı içeriyor. Ağların son aşaması anlamına gelen [uç noktalar](https://www.fortinet.com/products/endpoint-security/forticlient.html?utm_source=blog&utm_medium=blog&utm_campaign=endpoint-web-page), kullanıcıların en çok risk altında kaldığı yerleri oluşturuyor. Özellikle beyaz yakalı çalışanlar seyahatleri sırasında gündemi ve işleriyle ilgili haberleri takip etme ihtiyacı duyuyorlar. 2022’de yapılan bir araştırmaya göre insanların yüzde 82’si haberleri takip etmek için internet kullanıyor. Bu yüzden seyahat sırasında haber takibi yapmak için çeşitli lokasyonlardan internete erişen kullanıcılar cihazlarında daha fazla virüs bulundurma ihtimaline sahip. Örneğin kullanıcı cihazını seyahat sonrası kendi ortamında kullanmaya devam ediyor ve öncesinde birçok ağa ve aygıta bağlanmış olan cihaz kullanıcının kendi sunucularına bağlı ağına geri döndürüyor. Bu durumda eğer cihaza virüs bulamışsa, bu virüs kullandığı kurumsal ağa da bulaşma ihtimali taşıyor.

2022 yaz aylarında, insanların farklı bölgelere tekrar seyahat etmesinden yararlanan birçok farklı [kimlik avı](https://www.fortinet.com/resources/cyberglossary/phishing?utm_source=blog&utm_medium=blog&utm_campaign=phishing) saldırısı olduğu tespit edildi. [2022](https://www.fortinet.com/blog/threat-research/threat-actors-prey-on-eager-travelers?utm_source=blog&utm_medium=blog&utm_campaign=threat-actors-prey-on-eager-travelers) Haziran ayında Fortinet tarafından yayınlanan [tehdit raporunda](https://www.fortinet.com/blog/threat-research/threat-actors-prey-on-eager-travelers?utm_source=blog&utm_medium=blog&utm_campaign=threat-actors-prey-on-eager-travelers), seyahat programı hakkında bilgi sahibiymiş gibi davranan zararlı kodlar yüklü PDF dosyaları içeren kimlik avı dolandırıcılıklarından bahsediliyor. Bu tür saldırılarda havaalanları ve konferanslar son derece popüler lokasyonlar arasında yer alıyor.

**Seyahate çıkanlar kendilerini siber saldırılara karşı korumak için neler yapabilir?**

* En önemli nokta sistemlerin [yamalanması](https://www.fortinet.com/blog/business-and-technology/ukraine-crisis-cyber-readiness-checklist). Akıllı telefonlardaki uygulama mağazasından uygulamaların düzenli olarak güncellenmesi gerekir. Güncellemelerin nedeni çoğu zaman, güvenlik özellikleriyle veya düzeltilmiş bir hatayla ilgilidir. Bu uygulamalar güncellenmezse siber saldırganlar bu açık ve hatalardan faydalanabilir.
* Cihazların seyahat sırasında farklı kişilerle paylaşılmaması alınması gereken öncelikli önemlerdendir. Başka bir kullanıcı e-postasını sizin cihazınızdan kontrol etmek istediği halde zararlı bir dosyayı indirip cihaza zarar verebilir.
* Cihazların kilidini yabancıların yanında açık bırakılmamalıdır ve olabildiğince karmaşık parola oluşturulmalıdır. Karmaşık parolaları oluşturmak akılda tutmakta zorluk yaratabileceği için [şifre yöneticisi](https://www.fortinet.com/resources/cyberglossary/identity-and-access-management?utm_source=blog&utm_medium=blog&utm_campaign=identity-and-access-management) kullanmak kullanıcı için büyük kolaylık sağlayabilir. Şifre yöneticisi sayesinde kullanıcılar karışık hesap şifrelerini akıllarında tutmak zorunda kalmaz ve aynı zamanda şifrelerin güvenliğini sağlamış olur.

**Çalışanlar seyahat ederken ve iş için önemli ağlara bağlanırken uzaktan çalışmada nelere dikkat etmeli?**

* Çok zorunda kalınmadıkça halka açık alanlarda [Wi-Fi](https://www.fortinet.com/products/wireless-access-points?utm_source=blog&utm_medium=blog&utm_campaign=wireless-access-points)’a bağlanılmaması alınabilecek en önemli ve güvenli önlemlerdendir. Halka açık alanlardaki Wi-Fi ağlarına bağlanıldığında güvenliği zayıf olan bir ağ ise, kullanıcı, cihaz sisteminin diğer kişiler tarafından taranmasına olanak sağlayabilir. Bu durumda alınabilecek en büyük önlem kullanıcının kendi hotspot’unu oluşturmasıdır.

**Seyahatlerde sosyal medya çok daha sık kullanılıyor. Siber dünyada güvende kalmak için çalışanlar sosyal medyayı kullanırken nelerden kaçınmalı?**

* Birçok internet platformuna sosyal medya hesapları üzerinden giriş yapmak güvenlik riskini oldukça arttıran bir hatadır. Örneğin, bazı Wi-Fi’lara bağlanıldığında, hesap oluşturulması istenir veya başka platformlar üzerinden giriş yapma seçeneği sunulur. Sosyal medya hesaplarıyla giriş yapıldığı durumda, çoğu zaman platformu çalıştıranların birçok hassas bilgiye erişimine izin verilir.
* Günümüzde QR kodları hayatın her alanında kullanılmaya başlandı. Pandemi dönemiyle birlikte artık fiziksel temasın azaltılması için birçok restoranın tamamen QR menüye geçmesi buna verilebilecek en iyi örneklerdendir. QR kod genel anlamda hem kullanıcıya hem de üreticiye kolaylık sağlasa da, QR kodları taramanın potansiyel risk taşıdığı akıldan çıkarılmamalıdır. Genelde bir QR kod tarandığında, cihaz kullanıcıyı bir web sitesine yönlendirir. Bu web sitesi açıldığında, kullanıcının cihazına zararla dosyalar indirebiliyor ve güvenliğini ihlal edebiliyor.

**İlgili Kişiler**
İzel Bostancı - Marjinal Porter Novelli
0545 565 63 59
izelb@marjinal.com.tr
Beril Pelesen - Marjinal Porter Novelli
0537 220 49 39
berilp@marjinal.com.tr

**Fortinet hakkında**

İnsanları, cihazları, uygulamaları ve verileri her yerde koruma misyonuyla faaliyet gösteren Fortinet, güvenilir bir dijital dünya yaratmayı mümkün kılmaktadır. Bu yüzden dünyanın en büyük şirketleri, hizmet sağlayıcıları ve kamu kurumları dijital dönüşümlerini güvenle hızlandırmak için Fortinet’i tercih etmektedir. Fortinet Security Fabric, tüm dijital saldırı zemininde kapsamlı, entegre ve otomatik koruma sunarak kritik cihazları, verileri, uygulamaları ve veri merkezi, bulut ve home ofis arasındaki bağlantıyı korumaktadır. Fortinet global çapta sevkiyatı yapılan en güvenilir çözümler alanında dünyanın bir numarasıdır ve dünya genelinde 530 binden fazla müşteri ticari faaliyetlerini korumak için Fortinet'e güvenmektedir. Fortinet’in Training Advancement Agenda (TAA) inisiyatifinin bir parçası olan Fortinet NSE Eğitim Enstitüsü, herkesin siber eğitimlere erişebilmesi ve yeni kariyer fırsatlarını değerlendirebilmesi için sektördeki en büyük ve kapsamlı siber güvenlik eğitim programlarından birini sunmaktadır. Daha fazla bilgi için: https://www.fortinet.com, Fortinet Blog sayfası veya FortiGuard Labs.