**BASIN BÜLTENİ**

**Fortinet Çocukları Çevrimiçi Dünyada Güvende Tutmanın İpuçlarını Açıkladı**

***Pandemiyle gelişen eğitim koşulları, çocukların çevrimiçi dünyada her zamankinden fazla zaman geçirmesine neden oluyor. Bu noktada ebeveynler için çocuklarını bu dünyadan kaynaklanan tehditlere karşı güvende tutmak kritik hale geliyor. Fortinet ebeveynlere, çocukları güvende tutmaları için önemli ipuçları veriyor.***

Pandemiyle geçen bir yılın ardından birçok yetişkin evden çalışmaya, çocuklar ise uzaktan öğrenme yöntemleriyle eğitimlerini evden yürütmeye devam ediyor. Uzaktan eğitim günlük hayatın önemli bir parçası haline gelmiş durumda. Bu noktada ebeveynler için çocukları çevrimiçiyken güvende tutmanın farklı yollarını bilmek kritik hale geliyor.

NSE Eğitim Enstitüsü ile siber saldırılara karşı farkındalığı yaymak için çalışmalarını sürdüren Fortinet, online eğitimlerini sürdürüyor. Bu çabanın bir parçası olarak Fortinet CISO’su Renee Tarun tarafından “Bir Köpeğin Ağzından İnternet Güvenliği Kılavuzu” ([Cyber Safe: A Dog's Guide to Internet Security](https://go.fortinet.com/namer-lp/4x4pj?utm_source=referring-domain&utm_medium=cso-online&utm_campaign=CyberSafeBookPromo-NAMER-US&source=Other&Lead_Source_Most_Recent=Other)) adlı kitap kaleme alındı. Kitap internet güvenliği ile ilgili ebeveynler ve çocuklar için önemli ve dikkat çekici önerileri bir araya getiriyor.

**Çocukları çevrimiçi dünyada güvende tutmak için öneriler**

Uzaktan eğitim ile öğrenciler günlerinin büyük bir çoğunluğunda ev ağlarına bağlanıyorlar. Sanal derslerini bitiren çocuklar daha sonra televizyon programları izliyor, video oyunları oynuyor veya sosyal medyada geziniyor, yani genellikle dersten sonra da çevrimiçi kalıyorlar. Siber suçlular ise ev ağlarına bağlanan yeni cihazların sayısının artmasıyla fidye yazılımı saldırılarında bulunmak, bilgi çalmak için belirli cihazları hedefleyip devletin eğitim alanındaki güvenlik savunmalarını tehlikeye atmak için açık bir fırsat belirliyor ve bundan yararlanıyor. Bu nedenle, küçük yaşlardan itibaren internet güvenliği hakkında eğitim yoluyla çocuklar için siber farkındalık temeli oluşturmak kritik öneme sahip.

Uzaktan çalışanlar ise genellikle çevrimiçi tehditlerden korumak için kullandıkları cihazın ve ağın güvenliğine güveniyor. Ne var ki bu güvenlik çözümleri ancak bir noktaya kadar yarar sağlayabiliyor. Temel siber güvenlik uygulamaları hakkında bilgi sahibi olmak, iyi bir güvenlik duruşu edinmek uzun bir yol kat etmeyi gerektirebilir. Aynı şey, genellikle zamanlarının çoğunu çevrimiçi geçiren gençler için de geçerli. Ebeveynler, çocuklarına çevrimiçi güvenlik uygulamalarını anlatmalı, çocuklarının çevrimiçiyken karşılaşabilecekleri tehlikelerin farkında olmalarını sağlamalı. Ebeveynler şu konulara odaklanmalı:

* Çocuklar, aile ve arkadaşlarının gerçek adlarını, adreslerini veya diğer kişisel olarak tanımlanabilir bilgilerini (PII) çevrimiçi olarak yabancılarla paylaşmamalı; kişisel bilgilerini çevrimiçinde gizli tutmalı.
* Çocuklar ve gençler için açık kurallar belirlenmeli. Örneğin onaylanmış web sitelerinin ve uygulamaların listeleri oluşturulmalı veya belirli etkinliklerin ebeveyn onayını gerektirdiği anlatılmalı.
* Çocukların çevrimiçi olarak kimlerle iletişim kurduğu ebeveynler tarafından bilinmeli. Çocuklar, internette tanıştıkları biriyle asla yüz yüze görüşmemeleri gerektiğini iyi anlamalı.
* Sahte veya kötü amaçlı web sitelerine ve kimlik avı girişimleri gibi olası dolandırıcılıklara karşı dikkatli olma konusunda ebeveynler çocuklarıyla konuşmalı. Çocukların şüpheli bir bağlantıya tıklamaması veya beklenmeyen ekleri açmaması gerektiği açıkça belirtilmeli.
* Çocuklar ve gençler, internette buldukları bir şeyden emin değillerse, belirli bir web sitesi veya etkileşim hakkında endişeleri varsa güvenilir bir yetişkine sormaya teşvik edilmeli.
* Ailedeki herkesin parolalarının güçlü olması çok önemli. Anlamı açık olmayan veya kolayca erişilemeyen, güçlü, farklılaşmış parolalar kullanılmalı. Kullanmaktan kaçınılması gereken parolalara örnek olarak şunlar verilebilir: doğum günleri, cihazların otomatik verdiği varsayılan parolalar, kullanıcının adı veya basit sayı veya kelime kombinasyonları (yani 1234, password).
* Çalışırken veya evden online eğitim alırken cihazların güncel tutulması çok önemli. Tüm cihazların ve uygulamaların yamalarla tam olarak güncel olduğundan ve cihazdaki koruma yazılımının güncel ve çalışır durumda olduğundan emin olunmalı.

**Fortinet siber farkındalık kültürüyle çocukları bilinçlendiriyor**

Fortinet aynı zamanda siber güvenlik yetkinliği kazanmak isteyen herkes için NSE Eğitim Enstitüsü aracılığıyla ücretsiz siber farkındalık kursları (NSE 1 ve NSE 2) sunuyor. Bu kurslara küçük çocuklar da dahil olmak üzere tüm yaş grupları dahil olabiliyor. NSE Eğitim kursları, çocuk kitabında verilen bilgileri tamamlayarak, çocukların kötü aktörler hakkında bilgi edinmeleri ve öğrenmelerini NSE 1 ve NSE 2 seviyeleri aracılığıyla test etmeleri için temel siber farkındalık kursları sağlıyor.

**Fortinet Hakkında**

Fortinet dünya genelinde büyük ölçekli şirketlere, servis sağlayıcılarına ve kamu kurumlarına güvenlik sunar. Fortinet, her geçen gün büyüyen saldırı zemininde müşterilerine eksiksiz görünürlük ve kontrol sağlar, günümüzde artan ve gelecekte de artacak olan performans ihtiyaçlarını karşılamak için onları güçlendirir. Ağlardaki uygulamaların, çoklu bulut sistemlerinin ve sınır ortamlarının karşılaştığı en kritik güvenlik sorunlarına karşı tek çözüm olan Fortinet'in Security Fabric platformu, tüm dijital altyapıda veriyi korur. Fortinet global çapta sevkiyatı yapılan en güvenilir çözümler alanında dünyanın bir numarasıdır ve dünya genelinde 480 binden fazla müşteri ticari faaliyetlerini korumak için Fortinet'e güvenmektedir. Hem bir teknoloji şirketi hem de öğrenen bir şirket olan [Fortinet Network Security Expert (NSE)](https://training.fortinet.com/?utm_source=blog&utm_campaign=2019-q3-nse-institute) Eğitim Enstitüsü, sektördeki en büyük ve kapsamlı siber güvenlik eğitim programlarından birini sunmaktadır. Daha fazla bilgi için: [http://www.fortinet.com](http://www.fortinet.com/), [Fortinet Blog](https://blog.fortinet.com/) sayfası veya [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs?utm_source=pr&utm_campaign=FortiGuardLabs" \t "_blank).