Sosyal Ağlar
Ebeveyn Kılavuzu

ENJOY SAFER TECHNOLOGY

Giriş

Çocukların çoğunlukla dışarıda oynadığı ve sadece acıktıklarında eve geldikleri zamanların üzerinden çok geçmedi. Ama internetin hızlı yükselişi her şeyi değiştirdi. Günümüzde gençler dışarı çıkmak yerine günde birkaç saatlerini sosyal ağların sanal gerçekliğinde harcıyorlar.

ESET olarak bizler de birer ebeveyniz ve çocuklarınızın siber dünyanın içine çekildiğini görmekten duyduğunuz endişeyi anlıyoruz. Bu nedenle size bu kılavuzu sunuyoruz. Kılavuzda sosyal ağlarda gizlenen tehditlerin yanı sıra ailenizi ve çocuklarınızı korumanıza yardımcı olacak çözümler hakkında da bilgiler bulacaksınız.

1. Neye dikkat etmeli?

Kötü Amaçlı Yazılım

Kötü amaçlı yazılım tanımının İngilizcesi (malware), "malicious" (kötü amaçlı) ve "software" (yazılım) sözcüklerinin birleşiminden oluşur, başka bir deyişle zararlı kod anlamına gelir. Virüsler, solucanlar ve truva atları bilinen örneklerden bazılarıdır; bunların yaş sınırlaması olmaksızın kullanıcılara yaptıkları saldırılar teoride ve "doğal ortamda" zengin bir şekilde belgelenmiştir.

Bunlardan biri olan Koobface solucanı, 2009 yılında Facebook'ta yayılıyordu. Çekici mesajlar kullanarak kurbanının bilgisayarlarını botnet'in (saldırganın uzaktan kontrol edebildiği bilgisayarlardan oluşan bir zombi ordusu) bir parçası haline getiriyordu. İki yıl sonra ortaya çıkan yeni sürümü daha da gelişmişti; işletim sistemi Windows, Mac veya Linux'tan hangisi olduğu fark etmeksizin sosyal ağ kullanıcılarının cihazlarına virüs bulaştırıyordu.

E-Dolandırıcılık

Birçok saldırgan, çocuğunuzun sosyal ağ profilinin giriş bilgileri gibi hassas bilgileri çalmak için bu yöntemi kullanır. Genellikle sosyal medya web sitesinin bir kopyasının bağlantısını içeren e-posta yoluyla yapılır. Farklılıklar genellikle küçük olduğundan ve tuzağa düşen çocuklar bir gariplik olduğunu bile anlamadan bilgilerini girebileceğinden, sahte sayfayı tanımlamak oldukça zor olabilir.

Kimlik Hırsızlığı

Çocuklarınızın ev adresleri, cep telefonu numaraları, gittikleri okullar ya da dersler, doğum günleri veya teşhis edilmelerine neden olacak diğer veriler gibi hassas bilgiler yayınlamadıklarından emin olun. Bunun nedeni, siber suçluların kişisel bilgilerinizi ele geçirip sizi ve hatta çocuğunuzu kötü amaçlarına alet etmek için kullandıkları, siber suçların yaygın biçimlerinden biri olan kimlik hırsızlığıdır.

Saldırganın bu hassas verileri alabileceği iki ana yol vardır:

İlki, sosyal mühendislik yaparak çocuğunuzun bir arkadaşı veya onun yaşlarında biri gibi davranıp bu sırada kişisel bilgileri ortaya çıkarmaya çalışmaktır.

İkincisi ise yanlış ağ ayarlarıdır, bunlardan dolayı çok fazla bilgiye çocuğunuzun sosyal ağ profilinden doğrudan erişilebilir. Bunun sadece gençlerin değil, aynı zamanda risklerden habersiz birçok yetişkin kullanıcının da sorunu olduğunu unutmayın.

Çevrimiçi Gizli Takip ve Taciz

Kızınız veya oğlunuza yönelik sosyal ağlardaki tüm tehditler, siber suçlulardan gelmez. Arkadaşları da sorun olabilir. Bunu söylememizin nedeni zorbalığın artık sadece okul ve sınıfları ilgilendiren bir şey olmaması. Zorbalık günümüzde siber dünyaya taşındı ve her zamanki kadar zararlı.

Diğer bir sorun ise özellikle küçük çocukları hedef alan tacize hazırlamadır. Bu, bir yetişkinin çocuk gibi davranarak kolayca güven kazanması ve çocukları cinsel aktiviteler yapmaya ikna etmesi şeklinde tanımlanır. Çocuğunuza gönderilen veya onun gönderdiği uygunsuz cinsel içerikli mesajlarla bağlantılı birçok şekilde yapılabilir.

2. Hangi karşı önlemleri alabilirim?

Bu tehdit senaryolarında, sosyal ağların kullanımı gerçekten tehlikeli bir aktivite gibi görünüyor. Yine de, çocuğunuzun bunu kullanmasını yasaklamak, büyük olasılıkla bu sorunu çözmeyecek ve sadece belirlediğiniz kuralların delinmesine yol açacaktır. Ancak endişelenmeyin. Aşağıda, sosyal ağ kullanımını daha güvenli hale getirerek çocuklarınız ve aileniz için yeterli koruma sağlayacak ipuçlarını bulacaksınız.

Konuşun

Diyalog, özellikle konu sosyal ağlar olduğunda, çocuklarınızı çevrimiçi ortamda güvende tutmanın en önemli unsurlarından biridir. Çocuklarınızın kararınıza güvenmesini ve tavsiyelerinizi uymasını istiyorsanız, kanalları ve zihninizi sorulara ve tartışmaya açık tutmak çok önemlidir.

Siber zorbalık ve bunun önlenmesi buna iyi bir örnektir. Kızınıza veya oğlunuza, bu tür bir davranışla karşılaştıkları takdirde doğrudan onları ilgilendirmese bile (nerede olduğuna bağlı olarak) size, öğretmenine veya eğitmenine hemen haber vermeleri gerektiğini açıkça belirtin. Elinizdeki tek kanıt olduğundan zorbalık mesajını sakın silmeyin.

Ebeveyn kontrol yazılımı kullanın

Çocuklarınızın yaşına bağlı olarak ebeveyn kontrol yazılımından ve özelliklerinden yararlanın. **ESET Internet Security,** engelleyeceğiniz web sitelerinin listesini oluşturmanıza ve ayrıca çocuğunuzun çevrimiçi olarak harcayabileceği zaman ve saat miktarını kısıtlamanıza olanak tanır.

Diğer yandan, çocuklar da söz hakkına sahip olmalıdır. Bu nedenle **ESET Parental Control for Android,** tüm işlerini ve ev ödevlerini beklenenden daha önce bitirdikleri takdirde çocukların belirli bir web sitesini ziyaret etmek veya sosyal ağda geçirdiği süreyi uzatmak için izin istemelerine olanak sağlar.

Güvenilir bir güvenlik çözümü kullanmak

Kötü amaçlı yazılımlar siber dünyadaki en yaygın tehditlerden biri olduğundan, sosyal ağları kullanırken virüslerden kaçınmak için proaktif algılama yeteneklerine sahip bir virüsten korunma yazılımı ve çocuğunuzun cihazlarına güncel bir imza veritabanı kurmak gerekir.

İstenmeyen e-postaları engelleme ve güvenlik duvarı araçları da bu riskler karşısında sistem güvenliği optimizasyonunu mümkün kılar. Ayrıca çocuğunuz sosyal ağlarda gezinirken asla bir yönetici hesabı kullanmamalıdır. Güvenlik sorunlarının etkisini en aza indirmek için çocuklarınız için özel bir kullanıcı profili oluşturun.

Https kullanımını ayarlayın

Çocuğunuzun sosyal ağları kullanırken https protokolü (bunu web sitesinin adını yazdığınız adres çubuğunda görebilirsiniz) ile gezindiğinden emin olun. Bunu yapmak, okunabilir metin bilgilerine karşı gizli saldırılardan kaçınmanıza yardımcı olur. Https protokolü kullanılırken yalnızca çocuğunuzun kullanıcı adı ve şifresi değil, tüm veriler şifrelenir ve herhangi bir kötü amaçlı aktör tarafından okunamaz.

Sosyal ağlara genel Wi-Fi bağlantısından erişirken de bu faydalı ayarları kullanmaları konusunda çocuklarınıza tavsiyelerde bulunun.

Güçlü parolalar ve iki faktörlü doğrulamayı kullanın

Güvenli bir parolanın nasıl olduğunu çocuklarınız biliyor mu? "parola" veya "12345" gibi tahmin edilmesi kolay seçenekleri kullanmadıklarından emin olun. Ayrıca şifre en az 10 karakter uzunluğunda olmalı, büyük ve küçük harf, sayı ve # veya @ gibi özel bir sembol içermelidir. Parolalarını hiç kimseye, hatta en iyi arkadaşlarına bile vermemelerini hatırlatmayı da unutmayın.

Çocuklarınızın Facebook, Twitter veya diğer popüler sosyal ağlara bağlanırken güvenlik ayarlarında sunulan iki faktörlü doğrulamayı kullandığından emin olun. Akıllı telefonlarına tek kullanımlık bir parola gelmesi, saldırganlar için kırması zor olan başka bir güvenlik katmanı ekler.

Sosyal ağlarda doğru gizlilik ayarlarını kurun

Varsayılan sosyal ağ gizlilik ayarları çocuğunuzun güvenliğini garanti etmez. Bu nedenle ayarları doğru bir şekilde yaparken yeterli zaman ayırmanız ve hangi bilgilerin sızabileceğini kontrol etmeniz önerilir. Ne demek istediğimizi göstermek için örnek olarak Facebook'u kullandık:

Facebook

Çocuğunuzun profilindeki hiçbir profil ayarının istisnasız herkese açık olmadığından emin olun. Tercihen, bilgileri sadece arkadaşlarına, eğer arkadaşları çok fazla ise sadece küçük bir gruba (aile veya yakın arkadaş gibi) erişilebilir hale getirin.

Çocuğunuzun etiketlendiği resim, durum ve diğer içerikleri görebilecek kişileri sınırlayın. Uygulamaların kendi kişisel bilgilerine erişmesini veya duvarlarında gönderim yapmasını engelleyin.

Sadece kişisel olarak tanıdıkları insanlardan gelen arkadaşlık tekliflerini kabul etmelerini öğretin. Ayrıca siber dünyada yabancılarla konuşmanın veya iletişim kurmanın, gerçek dünyada olduğu kadar tehlikeli olabileceğini belirtin.

Çocuklarınıza Etkinlik günlüğünü kullanarak profillerini nasıl yönetebileceklerini, eylemlerini ve onlara bağlı olan diğer kişilerin eylemlerini nasıl gözden geçireceklerini gösterin. Daha detaylı bilgi için blog yazımızı okuyun: http://blog.eset.com/2011/05/25/facebook-privacy

Twitter

Twitter'ın, 140 karakterlik tweet limiti veya kısaltılmış URL'lerin sık kullanımı gibi kendine has özellikleri vardır. Çocuğunuza nasıl güvende kalacağını açıklarken bu farklılıkları da dikkate almanız gerekir.

Sadece tanıdıkları kişileri takip etmek ve şüpheli bağlantılardan kaçınmak gibi şeylere ek olarak, alabilecekleri şüpheli mesajların yasallığını da kontrol etmeleri gerekir. Bunlar kötü amaçlıysa, parçalarını araştırdıklarında büyük olasılıkla birisinin aldatmacayı keşfetmiş ve bunu ağa duyurmuş olduğunu görebilirler.

Ayrıca bilgisayarlarına veya cihazlarına kısa URL adreslerini çözen ve çocuklarınızın üzerine tıklamasına gerek kalmadan orijinal bağlantıyı görmesine izin veren bir tarayıcı eklentisi yükleyin.

Diğer sosyal medya ortamları

Çocuğunuz Snapchat, Instagram veya YouTube gibi diğer sosyal medya ortamlarını tercih ediyor mu? Özellikle bu ağlar için özel olarak hazırlanmış diğer video kılavuzlarımıza da bakın. Ayrıca listemizde yer alan, çocuklar için daha uygun sosyal ağlardan birini de seçebilirsiniz.

3. Sonuç

Şüphesiz ki, sosyal ağlar İnternet kullanıcıları için değerli bir kaynaktır. Yine de bu kılavuzun gösterdiği gibi, çocukların kullanırken maruz kalabilecekleri birçok tehdit vardır. Bu nedenle siber suçluları veya diğer kötü amaçlı aktörleri hafife almayın ve hayatınızdaki en değerli insanları korumak için BT araçlarından iyi bir şekilde faydalanın.

Sosyal ağ profillerini düzgün bir şekilde ayarlamalarına yardımcı olmak ve basit ama yararlı öneriler sunmak, onları güvenli tutmak konusunda yapılacak en önemli şey olabilir.

Not:

Bu kılavuzda verilen tavsiyelerin çoğunu hatırlamak istiyorsanız Cyberspace Safety Decalogue (Siber Dünya Güvenliğine Dair On Tavsiye) adlı daha kısa ve basit versiyonu uygulayabilirsiniz:

1. Şüpheli bağlantılardan kaçının

2. İtibarları şüpheli olan web sitelerine asla girmeyin

3. İşletim sistemini ve uygulamaları güncelleyin

4. Uygulamaları sadece resmi web sitelerinden indirin

5. Güvenlik Teknolojisi kullanın

6. Şüpheli formlara kişisel bilgi girmekten kaçının

7. Web tarayıcılarının getirdiği sonuçlar konusunda dikkatli olun

8. Sadece tanıdığınız kişileri kabul edin

9. Şüpheli dosyaları çalıştırmayın

10. Güçlü şifreler kullanın