



Digital Security
Progress. Protected.

safer**kid**sonline

Sosyal Ağlar Ebeveyn Rehberi

Giriş

Çocukların sokakta oynadıkları ve eve sadece acıktıklarında geldikleri zamanı hatırlıyor musunuz? İnternet her şeyi değiştirdi. Bugünlerde gençler sosyal ağlarda her gün saatlerce zaman harcıyorlar.

ESET çalışanları olarak birçoğumuz ebeveyniz ve çocuğunuzun siber dünyanın içine çekildiğini görmekten duyduğunuz endişeyi anlıyoruz. İşte bu nedenle bu kılavuzu hazırladık. Kılavuzda sosyal ağlarda gizlenen olası tehditler ve ailenizi korumanıza yardımcı olacak çözümler hakkında bilgiler bulacaksınız.



1. Neye dikkat etmeli?

Kötü Amaçlı Yazılım

Kötü amaçlı yazılımın İngilizce karşılığı (malware), "malicious" (kötü amaçlı) ve "software" (yazılım) sözcüklerinin birleşiminden oluşur. Başka bir deyişle zararlı kod anlamına gelir. Virüsler, solucanlar ve Truva Atları örnek olarak verilebilir. Dolandırıcılar genellikle korsan yazılım ya da oyunlar vadederek kullanıcıları kötü amaçlı yazılım indirmeye ikna etmek için sosyal ağları kullanırlar.

Kimlik Avı

Kurbanları yakalamak amacıyla yem kullanıldığı için, kimlik avının İngilizce karşılığı olan "phishing" terimi, "fishing" (balık avı) teriminden türetilmiştir. Birçok saldırgan, çocuğunuzun sosyal ağ profilinin giriş bilgileri gibi hassas bilgileri çalmak için bu yöntemi kullanır. Bu genellikle sosyal medya web sitesinin bir kopyasının bağlantısını içeren e-posta yoluyla yapılır. Farklılıklar genellikle çok küçük olduğundan sahte sayfayı ayırt etmek oldukça zor olabilir ve çocuklar bir gariplik olduğunu bile fark etmeden bilgilerini girebilirler.

Kimlik Hırsızlığı

Çocuklarınızın kimliklerini saptamak için kullanılabilecek ev adresi, okul adresi, telefon numarası ya da doğum günü gibi hassas bilgileri yayınlamadıklarından emin olun. Kimlik hırsızlığı; siber suçluların, kullanıcıların kişisel bilgilerini ele geçirip kendilerini kötü amaçlarla taklit etmek için bu bilgileri kullandıkları yaygın bir siber suç türüdür.

Saldırganın bu hassas verileri alabileceği iki ana yol vardır:

Genellikle çocuğunuzun arkadaşı gibi görünmek suretiyle sosyal mühendisliği kullanma

Sosyal ağ profilinde herkesin erişebildiği bilgileri kullanma (uygun gizlilik ayarlarını seçmek hayati önem taşır)

Çevrimiçi Gizli Takip ve Taciz

Sosyal ağlarda çocuklarınıza yönelik tüm tehditlerde siber suçlular olmak zorunda değildir. Çocuklarınızın akranları da sorun olabilir. Zorbalık okul sınırlarını aşarak artık internete de yayıldı ve en az gerçek hayatta olduğu kadar zararlı olabiliyor.

Bir diğer ciddi sorun ise, özellikle küçük çocukları hedef alan istismara hazırlama eylemleridir. İstismara hazırlama, bir yetişkinin cinsel eylemler gerçekleştirmesi için bir çocuğun güvenini kazanmaya ve onunla bir ilişki kurmaya çalışmasıdır. Bu genellikle cinsel içerikli mesajları (çocuğunuza ya da çocuğunuz tarafından gönderilmiş olabilen, uygunsuz içeriğe sahip mesajlar) içerir.

2. Çocuklarınızı korumak için ne gibi önlemler alabilirsiniz?

Olası tehditlere bakıldığında, sosyal ağ kullanımı tehlikeli bir etkinlik gibi görünebilir. Ancak, çocuğunuzun bunları kullanmasını yasaklamak sorunu çözmez. Çocuğunuz her zaman istediğini elde etmenin bir yolunu bulacaktır. Aşağıda, sosyal ağ kullanımını daha güvenli hale getirecek ve hem çocuklarınız hem de aileniz için yeterli korumayı sağlayacak ipuçlarını bulacaksınız.

Konuşun

Diyalog, özellikle konu sosyal ağlar olduğunda, çocuklarınızı çevrimiçi ortamda güvende tutmanın en önemli unsurlarından biridir. Sizin yargılarınıza güvenmelerini ve önerilerinize uymalarını istiyorsanız çocuklarınızla açık ve dürüst iletişim kurmak çok önemlidir.

Siber zorbalık ve bu zorbalığı önleme çalışmaları buna iyi bir örnektir. Çocuğunuza bu tür bir davranışla karşılaştığı takdirde, doğrudan onu ilgilendirmese bile size, öğretmene ya da sorumlu diğer yetişkinlere hemen haber vermesi gerektiğini açıkça belirtin.

Ebeveyn kontrol yazılımı kullanın

Çocuğunuzun yaşına bağlı olarak, ebeveyn kontrol yazılımı kullanın. ESET Smart Security engellenen web sitelerinin listesini oluşturmanıza ve çocuğunuzun internete bağlanabileceği saatleri kısıtlamanıza olanak tanır.

Ancak, çocukların da söz hakkı olmalıdır. Bu nedenle, ev işlerini ya da ev ödevlerini beklenenden daha önce bitirme gibi durumlar söz konusu olduğunda, ESET Parental Control for Android çocukların belirli web sitelerini ziyaret etmek ya da sosyal ağda geçirdikleri süreyi uzatmak için izin istemelerine olanak sağlar.

Güvenilir bir güvenlik çözümü kullanmak

Kötü amaçlı yazılımlar siber dünyadaki en yaygın tehditlerden biri olduğundan, çocuğunuzun cihazlarına proaktif algılama özelliklerine sahip bir güvenlik çözümü kurmak, sosyal ağları kullanırken virüslerden kaçınmaları için büyük önem taşır.

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 çocuklarınıza özel bir kullanıcı profili oluşturun.

Güçlü parolalar ve iki faktörlü doğrulamayı kullanın

Güvenli bir parolanın nasıl olduğunu çocuklarınız biliyor mu? "parola" veya "12345" gibi tahmin edilmesi kolay seçenekleri kullanmadıklarına emin olun. Parola en az 10 karakter uzunluğunda olmalı, büyük ve küçük harf, sayı ve # veya @ gibi özel bir sembol içermelidir. Bir ifadeyi ya da şarkı sözünü uyarlamak işe yarayabilir:

Örneğin kırmızı balık, "Kırmızı1b@lık" şeklinde bir parolaya dönüştürülebilir.

Parolalarını hiç kimseyle, hatta en iyi arkadaşlarıyla bile paylaşmamaları gerektiğini hatırlatmayı da unutmayın.

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

Profil ayarlarını "özel" olarak değiştirin

Sosyal ağların varsayılan gizlilik ayarları, çocuğunuzun güvenliğini garanti etmez. Bu nedenle, biraz zaman ayırıp bu ayarları yapmanız ve hangi bilgilerin sızabileceğini kontrol etmeniz önerilir. Örnek olarak Facebook'u kullanalım:

Facebook

Hiçbir şeyin tüm kullanıcılarla paylaşılmadığından emin olmak için profil ayarlarını kullanın. Tercihen, bilgilerin sadece arkadaşlar ve aile üyeleri, hatta mümkünse sadece küçük gruplar (yakın aile ya da en iyi arkadaşlar) tarafından erişilebilir olmasını sağlayın.

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 internette yabancılarla konuşmanın ya da iletişim kurmanın, gerçek dünyada buluşmak kadar tehlikeli olabileceğini açıklayın.

Facebook ayarlarını kullanma hakkında ayrıntılı bilgi için lütfen blogumuzu okuyun: <http://blog.eset.com/2011/05/25/facebook-privacy>

Twitter

Twitter'ın, 280 karakterlik 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 hususlara ek olarak, alacakları mesajların doğruluğunu da kontrol etmeleri gerekir. Kötü amaçlı mesajlar genellikle diğer kullanıcılara ve paylaşılan bilgilere bakılarak saptanabildiği için mesajın bir bölümü kullanılarak yapılacak hızlı bir arama işe yarayabilir.

Ayrıca, çocuklarınızın bilgisayarına ya da cihazına, kısa URL adresine tıklamadan orijinal bağlantıyı görmelerini sağlayan, tanınmış bir tarayıcı eklentisi yükleyin.

Diğer sosyal medya ortamları

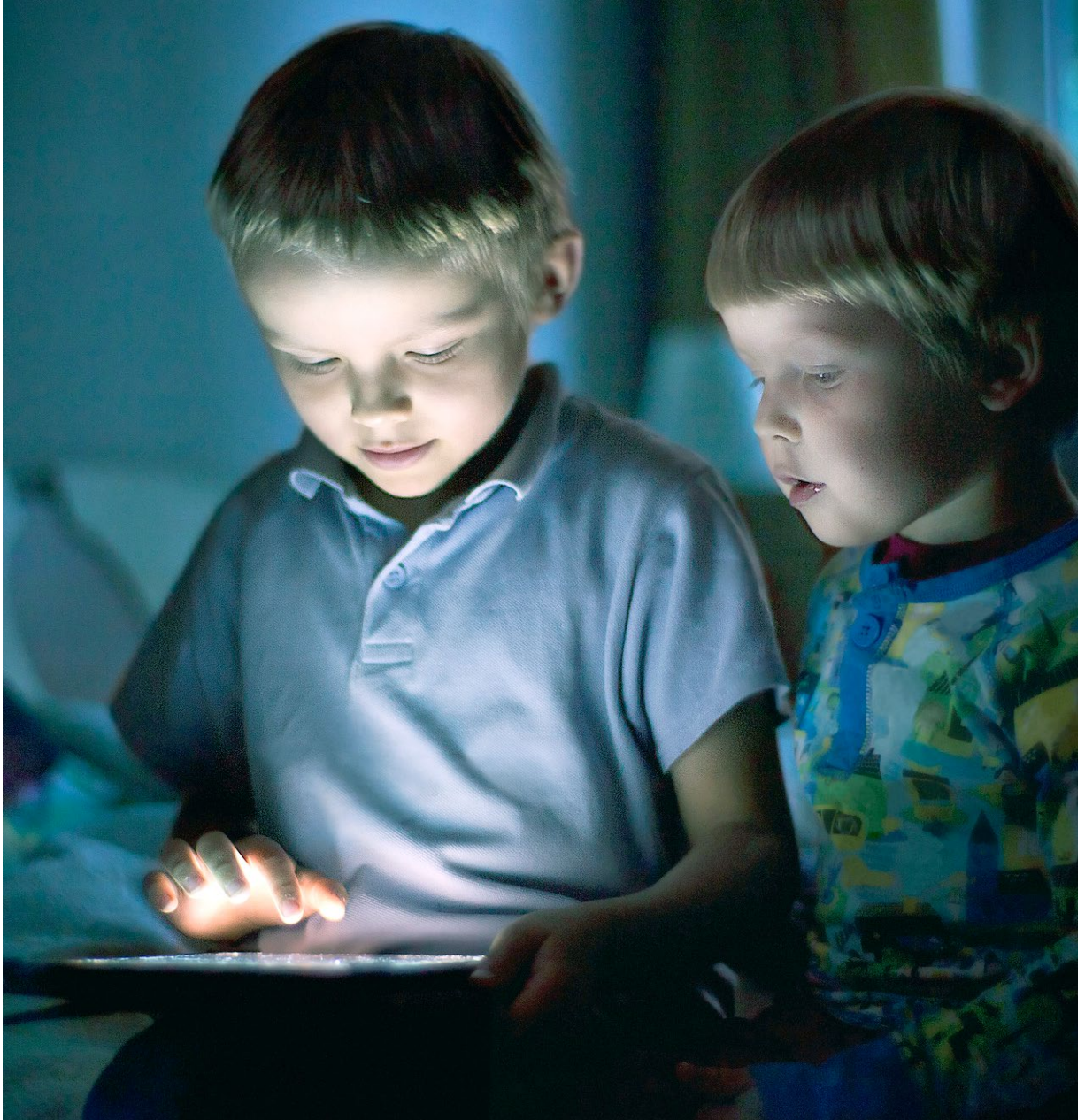
Farklı ilgi alanlarına ve yaş gruplarına hizmet veren birçok sosyal medya sitesi vardır. Çocuklarınızın kendilerine uygun olanları kullanıp kullanmadıklarını kontrol etmek önemlidir. Snapchat, Instagram ve YouTube'un ele alındığı video kılavuzlarımız bulunuyor. Ayrıca çocuklara uygun sosyal ağları da derleyerek bir liste haline getirdik.



3. Sonu

Sosyal aęlar internet kullanıcıları iin deęerli bir kaynak olabilir. Yine de bu kılavuzun gsterdięi gibi, ocukların kullanırken maruz kalabilecekleri birok tehdit vardır. Siber suluları ya da dięer kt amalı aktrleri hafife almayın. Hayatınızdaki nemli kiřileri korumak iin en iyi uygulamaları hayata geirmek ve gvenilir gvenlik aralarını kullanmak gerekir.

Sosyal aę profillerini dzgn bir řekilde ayarlamalarına yardımcı olmak ve basit ama yararlı neriler sunmak, onları gvende tutmak konusunda yapılacak en nemli řey olabilir.



En önemli 10 ipucu

1. Çocuklarınıza bağlantılara ve indirme düğmelerine tıklamadan önce durup düşünmeyi öğretin
2. Onlara çevrimiçi iletişime sağlıklı bir düzeyde dikkat ile yaklaşmayı öğretin
3. Çocuklarınızın hesaplarını özel moda alın
4. Onlara yabancılardan gelen arkadaşlık tekliflerini reddetmelerini öğretin
5. İşletim sistemlerinin ve güvenlik yazılımlarının güncel kalmasını sağlayın
6. İyi bir rol modeli olun ve kendi dijital kullanımınızı kontrol altında tutun
7. Bir çocuğun siber zorbalık kurbanı olduğunu gösterebilecek işaretlere dikkat edin
8. ESET Parental Control gibi tanınmış bir ebeveyn kontrol uygulaması kullanın
9. Onları güçlü parolalar kullanmaya teşvik edin
10. Kişisel bilgileri, videoları ya da fotoğrafları paylaşmadan önce düşünmelerini isteyin