İnternette Çocukların Korunması için Ebeveyn Kılavuzu

ENJOY SAFER TECHNOLOGY

Giriş

Çocuklar bizim en büyük varlığımız, geleceğimizdir. ESET olarak bizler de sizin gibi ebeveyn olduğumuz için bunu biliyoruz. Onlara yaşam boyunca rehberlik etmemiz ve onları zarar görmekten korumamız gerektiğini düşünüyoruz, ancak bu sorumluluk bugün büyük bir zorluğu da gözler önüne seriyor.

Giderek modernleşen ve karmaşık hale gelen mobil cihazlar ve hızla değişen bir dilden dolayı, çocuklarını eğitebilmek için önce kendilerini eğitmek söz konusu olduğunda ebeveynler üzerindeki baskı artar.

Bu kılavuz size yardım eli uzatmakta ve çocuklarınızın internette ve aslında siber dünyanın sunduğu her şeyde, sağlıklı ve güvenli bir deneyime sahip olmalarını sağlamak için hangi yönlerin dikkate alınması gerektiğini açıklamaktadır.

Onlarla kim konuşmalı?

Sizi rahatsız hissettirebilir fakat bu kişi siz olmalısınız.

Kızınız ya da oğlunuz çocukluğu boyunca akrabaları, arkadaşları ve öğretmenleri gibi hayatında çok önemli roller oynayacak olan insanlarla tanışacaktır.

Ancak hiçbiri ebeveyn olarak sizin rolünüzü üstlenemez. Bir çocuğun gözünde, tüm cevapları elinde bulunduran ve ne yapacaklarından emin olmadıklarında onlara yardım edebilecek olan kişi sizsiniz.

Onlarla ne zaman konuşmalı?

Şimdi. Veya mümkün olan en yakın zamanda.

Çocuğunuz büyüdükçe yeni sorunlar ortaya çıkar. Bu yeni durumlarda verilecek candan ve sevgi dolu bir tavsiye, çocuğunuzun gelecekte doğru yönde ilerlemesini sağlayacak belirleyici bir adım olabilir. Bu, özellikle siber dünya söz konusu olduğunda geçerlidir.

Çocuk; tablet, akıllı telefon veya bilgisayara ve internete ilgi göstermeye başladığı andan itibaren, genel olarak güvenlikle ilgili öğrendiği her şeyin web için de geçerli olduğunu açıklamaya başlamalısınız. Diğer bir ifade ile, araçlar değişmiş olsa da tehditler yerinde duruyor.

Ebeveynler hem çocuklarını eğitirler hem de onlardan öğrenirler.

Çocuklarınızın "bilgisayar teknolojisi hakkında sizden daha fazla bilgi sahibi olduklarını" mı hissediyorsunuz? Bu kompleksten muzdarip olan tek ebeveyn siz değilsiniz.

Günümüzde çocuklar dijital dünyanın adeta ellerinde akıllı telefon ile doğmuş yerlileri olmakla birlikte, birçok yetişkin bu becerileri ancak yaşamlarının sonraki kısımlarında kazanmıştır.

Yine de bu, çocuğunuzun evinizdeki tüm bilgi işlem gücüne sahip kişi olması gerektiği anlamına gelmez. İnternetin nasıl kullanılacağını bilmek, çevrimiçi ortamdaki herhangi bir eylemin sonuçlarını anlamakla aynı şey değildir.

Bir ebeveyn olarak, çevrimiçi dünyada olup bitenler hakkında çocuğunuzdan daha fazla bilgi sahibi olmanıza gerek yoktur.

Fakat çocuklarınızın alışılmadık bir şeye rastladıkları ve daha deneyimli biriyle konuşmaya ihtiyaç duydukları durumlarda kontrol sizde olmalı.

Burada önemli olan, çocuğu tartışmaya dahil etmektir. Bu nedenle, özgürce soru sorabilecekleri ve tüm yeni bilgileri kavrayabilecekleri bir ortam yaratın.

Çocuğum o yaşa geldiğinde ne yapmalı?

Aşağıda, çocukların çevrimiçi aktivitelerini yaşlarına göre daha güvenli hale getiren temel bir araç seti paylaşıyoruz.

10 YAŞINA KADAR

1. "Web'deki ilk deneyimleri sırasında onlara eşlik edin"

Çocuklarınız ilk adımlarını attığında yanlarında olun. Çocuğun internetle olan ilk teması, beraberce oturup ona yeni maceralarında rehberlik etmek için iyi bir fırsattır.

2. "İnternet kullanımı için koşulları belirleyin"

İnternet için temel kuralları belirleyin. Çevrimiçi geçirilen saat sayısını denetlemek ve ayrıca web kullanımına izin verilen zamanları belirlemek, iyi bir uygulamadır.

3. "İyi bir örnek olun"

Çocuklar genellikle ebeveynlerinin davranışlarını örnek alırlar; bu kural, gerçek hayatın yanı sıra çevrimiçi ortamlar için de geçerlidir. Ailenin üyeleri olumlu bir davranışa sahipse bu hemen çocuğa geçecektir.

11 İLA 14 YAŞ ARASI

1. "Ebeveyn kontrol araçları kullanın"

Var olan teknolojiden faydalanın ve bunu kendi yararınıza kullanın. ESET Parental Control araçları, sitelerin ve hatta rahatsız edici içeriğe sahip sayfa kategorilerinin engellenmesini mümkün kılar, internette gezinmek veya oyun oynamak için zaman sınırları belirlemenize olanak tanır. Aynı zamanda, ev ödevini yaptığı takdirde çocuğunuzun sizden belirli sayfaları ziyaret etmek veya oyun zamanını uzatmak için izin istemesine imkan verir.

2. "Onları teşhir edebilecek bilgileri paylaşmamayı öğretin"

Çevrimiçi dünyada herkesin arkadaş olmadığını ve bazı insanların onları incitmek isteyebileceğini çok açık bir şekilde belirtmek önemlidir. Adres, telefon, okul veya okuldan sonra katıldıkları aktiviteler gibi bilgileri paylaşmanın neden güvenli olmadığını açıklayın.

Çocuk internette hassas resimler paylaşmadan önce de sizden izin istemelidir.

3. "Diyalog kanallarını açık tutun"

Çocuklarınızı sizinle açık olmaya ve internette gördükleri şeyleri özgürce sormaya teşvik edin. Mümkünse bilgisayarı kendi odasına değil, tüm ailenin vakit geçirdiği bir odada ve gözetiminizde olabileceği bir yere koymaya çalışın.

15 İLA 18 YAŞ ARASI

1. "Parolalarını kimse öğrenmemelidir"

Ergenlik çağına girmiş çocukların nasıl olduklarını ve onlarla anlaşmanın gerçekten zorlaşabildiğini biliyoruz, ancak parolalar söz konusu olduğunda neyin doğru olduğunu bildiklerinden emin olun. Sonuçta parolalar da ev anahtarından farksızdır. Çocukların gizliliğine saygı gösterin, ancak aynı zamanda parolalarını bir yabancıya vermediklerinden ya da bizzat veya internet üzerinden başkalarına "ödünç" vermediklerinden emin olun.

2. "Taciz veya siber zorbalığı anında bildirin"

Sınıfınızdaki zorbaları hatırlıyor musunuz? Çalışkan öğrencilerin hayatını çekilmez hale getiren o büyük çocuğu? Günümüzde o çocukların çoğu modern teknolojiye geçiş yaptı ve internetin arkasına saklanıyorlar. Değişmeyen şey, başkalarına psikolojik olarak zarar vermeye çalışmaları.

Bu nedenle, çocuklara bu yanlış eylemlere rastladıklarında hemen ebeveynlerini bilgilendirmeleri söylenmelidir.

3. "Çevrimiçi finansal işlemler sadece yetişkinler içindir"

Dikkatli yapıldığı sürece internetten bir şey satın almak sorun olmaz. Kişisel finansal bilgileri gönderirken gerekli olan önlemleri anlayıncaya kadar çocuklar bunu yalnızca ebeveynlerinin gözetiminde yapmalıdırlar.

Siber Güvenlik Sözlüğü

"Okulda veya evde"

Ebeveyn olmak çocuğun siber güvenliği için çok önemli bir sorumluluk gerektirse de tüm bu yükü sadece sizin taşımanız gerektiği anlamına gelmez. Çocuğunuzun okulunda internet güvenliğine odaklanan dersler verilip verilmediğini kontrol edin. Hatta dersi sevilen bir öğretmen veriyorsa ebeveynlerini dinlemeyi reddeden genç için gerçekten güçlü bir rol modeli olabilir. Okul, çocuğunuza daha önce verdiğiniz siber güvenlik temellerinin üzerine, üst seviyeye taşınmış bir farkındalık inşa edebilir.

"Ebeveyn Kontrolü"

Çocuğunuzun internete erişim zamanlarını ve saatlerini ayarlayabileceğiniz, ziyaret edeceği sayfaların türlerini sınırlandırabileceğiniz, hangi oyunları oynayabileceğine izin verebileceğiniz veya yasaklayabileceğiniz veya çocuğun tam konumunu izleyebileceğiniz bir program olduğunu düşünün. Bu tür yazılımlara ebeveyn kontrolü adı verilir ve oğlunuzun veya kızınızın ne zaman çevrimiçi olduklarını kontrol etmek için size güçlü bir araç sunar.

Diğer yandan, bu onlara da bir söz hakkı sunmalıdır. Çünkü eğer kontrolleri olmadığını ve kısıtlamaların çok sert olduğunu düşünürlerse bu, sadece kuralları ihlal etmelerine neden olacaktır.

"Sosyal ağlar"

Tüm okul arkadaşlarınızı, dostlarınızı ve tanıdıklarınızı hatırlayın. Bir kısmını tek bir odaya koyun ve neler yaptıklarını anlattıklarını, size tatil resimlerini veya beğendikleri videoları gösterdiklerini düşünün. Bu aslında sosyal ağların bugünlerde nasıl çalıştığını özetler: Kullanıcıların etkinlikler organize etmesine, diğer insanlar ile bireysel veya bir grup içinde görüşmesine ve onların nelerden hoşlandıklarını görmesine imkan tanır.

Yarattığınız bu küçük mikro kozmos, sizin isteğinizle sizinle etkileşimde bulunan yüz milyonlarca kullanıcının oluşturduğu bir üst yapının yalnızca küçük bir kısmıdır. Ancak tüm bu faydalar yanında bazı riskler getiriyor.

Ana tehditler hangileridir?

Kötü Amaçlı Yazılım

Kötü amaçlı yazılımın İngilizcesi olan "malware", "malicious" (kötü amaçlı) ve "software" (yazılım) sözcüklerinin kısaltılmış halidir. Bu tür uygulamaların amacı, bilgisayara çeşitli şekillerde zarar vermektir. Bazıları bilgisayarınızdaki dosyaları şifreleyecek, diğerleri sizi gözetlemeye çalışacak veya bilgisayarınıza başka tehlikeli uygulamalar indirecektir.

Çoğu durumda virüs, saldırgan tarafından tuzağa düşürüldükten sonra kullanıcılar (veya çocukları) tarafından yapılan "hatalar" nedeniyle bulaşır. Saygın güvenlik çözümleri ve iyi uygulamalar, bu tür kötü amaçlı kodlardan etkilenme riskini azaltır.

İstenmeyen E-posta

İstenmeyen e-postaları daha önce görmüşsünüzdür. Bunlar her gün gelen kutunuzu dolduran "önemsiz e-postalardır." Bu tür iletilerde, sizi belirli sayfaları ziyaret etmeye davet eden ve çoğunlukla zararlı içerik barındıran "mucize" teklifler içeren reklamlar bulunur.

İnternet Dolandırıcılığı

İnternet dolandırıcılığı, internet üzerinden yapılan aldatmaya yönelik eylemlerdir. Sosyal mühendislik tekniklerinin yanı sıra istenmeyen e-posta gibi birçok şekle bürünebilirler.

İkinci durumda saldırganlar bir şey satmayı teklif eder, meslektaşlarınız gibi davranırlar ve hatta bankanızın kimliğine bürünürler. İstedikleri tek şey, gizli bilgi elde etmektir. Sosyal ağ kullanıcı adımızı ve parolamızı internet üzerinden isteyen sahte mesajlar da sıkça görülen bir internet dolandırıcılığı örneğidir.

Siber Zorbalık

Bu düşmanca davranış özellikle çocuklara yöneliktir. Mağdur genellikle siber dünyadaki akranları tarafından tehdit edilip aşağılanır ve buna gençler arasında sık rastlanır. Bu, çocuğa zarar verebilir ve duygusal bir travmaya neden olabilir. Siber zorbalık genellikle internet üzerinden gerçekleşir, ancak cep telefonlarının veya oyun konsollarının dan bu zararlı davranışlara karşı bağışıklığı yoktur.

İstismara hazırlama

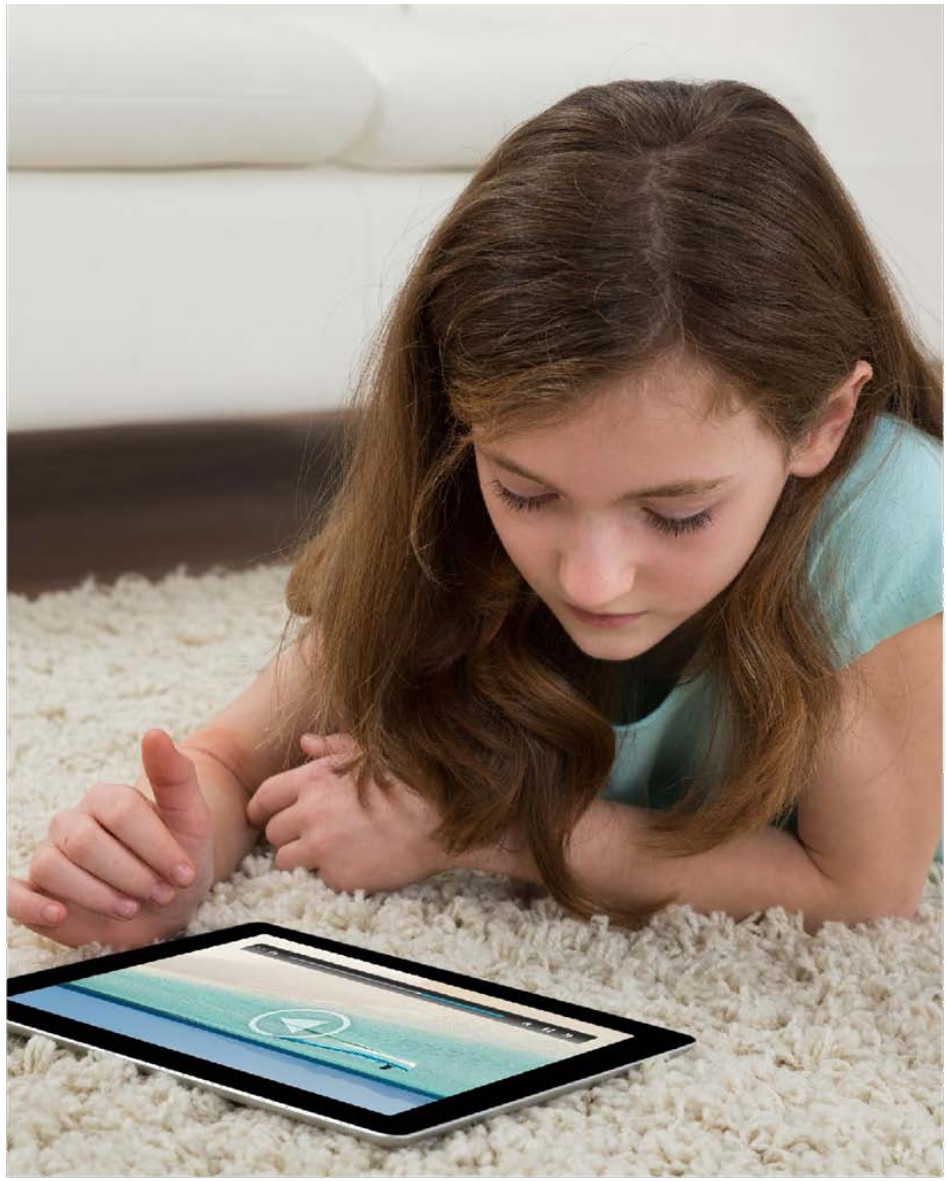
Bu, bir yetişkinin güven ortamı yaratarak ve duygusal bir bağ kurarak bir çocuğu cinsel aktiviteler gerçekleştirmek üzere ikna etmeye çalışmasıdır. Çoğu zaman yetişkinler yakın ilişki kurabilmek için çocukmuş gibi davranırlar ve sonra yüz yüze görüşme ayarlamaya çalışırlar. Bir ebeveynin, çocuğunun çevrimiçi ortamda etkileşimde bulunduğu kişilerin kimler olduğuna ilişkin yeterince bilgiye sahip olması önemlidir.

Cinsel İçerikli Mesajlaşma

Cinsel içerikli mesajlaşmanın İngilizcesi olan "Sexting", "sex" (seks) ve "texting" (mesajlaşma) sözcüklerinin kısaltılmasından oluşur. Adından da anlaşılacağı gibi bu, erotik mesajlar içeren e-postalar için kullanılan bir terimdi. Teknolojik ilerlemenin ardından görüntü ve video alışverişini de kapsayacak şekilde değişti ve çoğu gencin ve çocuğun mobil cihazlarını sürekli yanlarında taşıması nedeniyle yaygın bir uygulama haline geldi.

Bilgi Hırsızlığı

Web üzerinden geçen tüm bilgiler, gerekli önlemler alınmadığı takdirde üçüncü taraflarca yakalanabilir. Bu, çoğu zaman bir saldırı amacıyla yapılır. Hedef alınan bilgi genellikle sizin veya çocuğunuzun kişisel verileridir. Bu tür olaylarda yanlış bir adım atmak, çocuğun aile parasını kaybetmesine neden olabilir ya da en kötü durumda onu kimlik hırsızlıklarına maruz bırakabilir.



Son öneriler

1. Ebeveyn kontrol araçlarını kullanın

Bu araçlar hem tarayıcıda hem de antivirüs yazılımında kullanılabilir. Bunlar, ESET Smart Security'nin 9. Sürümünde veya ayrı bir uygulama olan ESET Parental Control for Android uygulamasında bulunabilir. Nintendo Wii ve Xbox 360 gibi oyun konsolları için de bu tür araçlar mevcuttur.

2. Çocuğunuzun internet üzerinden özel bilgiler göndermesine izin vermeyin.

Hassas bilgiler asla e-posta veya yazılı sohbet yoluyla istenmemelidir. Bankalar şifreleriniz şöyle dursun, hesap bilgilerinizi dahi bu şekilde talep etmezler. Böyle değerli bilgileri çocuğunuza vermemeniz gerekir.

3. Taciz mesajlarını yanıtlamayın ve yok etmeyin

Çocuğunuz siber zorbalık mağduru ise misilleme yapmamalıdır. Tacizcinin, zarar verme arzusunu beslemek amacıyla bu şekilde bir tepki uyandırmaya çalıştığını açıklayın. Bu tür durumlarla karşılaşırsanız ve bunlar tekrar ederse ilgili makamlara haber verin. Ancak gelmiş hiçbir mesajı silmeyin çünkü gerektiğinde eylemin delili olarak gösterebilirsiniz.

4. Çevrimiçi ortamda gördüğünüz her şey doğru değildir

İnternette bulunabilen tüm bilgiler güvenilir bir kaynaktan gelmez ve çocuk bu farkı bilmelidir. Çevrimiçi ortamda bir yer edinme ve içerikleri manipüle etmenin ne kadar kolay olduğunu göstermek için fikirlerinizi yazabileceğiniz bir blog oluşturun.

5. Açık diyalog

Çocuklarınızla iletişiminiz onların güvenliğinde önemli bir rol oynar. Onları korku ve endişeleri hakkında konuşmaları için teşvik etmek, cezalandırmaktan çok daha verimli sonuçlar doğurur. Hem internette hem de gerçek hayatta iyi bir çevre ve açık diyalog, onların iyiliği için uğraşırken başarıya götüren anahtar olabilir.

6. Eğer bir şeyi çevrimiçi ortamda yayınlarsanız, orada sonsuza kadar kalır

Çocuklarınıza, çevrimiçi ortamda yayınladıkları herhangi bir şeyin sonsuza kadar orada kaldığını öğretin. Üstelik başkaları ve hatta yabancılar tarafından paylaşılabildiği için, yayınladıklarının üzerindeki kontrolü de kaybederler. Pratik kural, sizin veya büyükannelerinin görmelerini istemedikleri bir fotoğrafı, durum bilgisini veya diğer içerikleri paylaşmamaktır.

Bu; sosyal ağlar, anlık mesajlaşma platformları, bloglar veya yorumlar olmak üzere her tür çevrimiçi varlık gösterme şekli için geçerlidir.

Ebeveynler için 5 ipucu daha

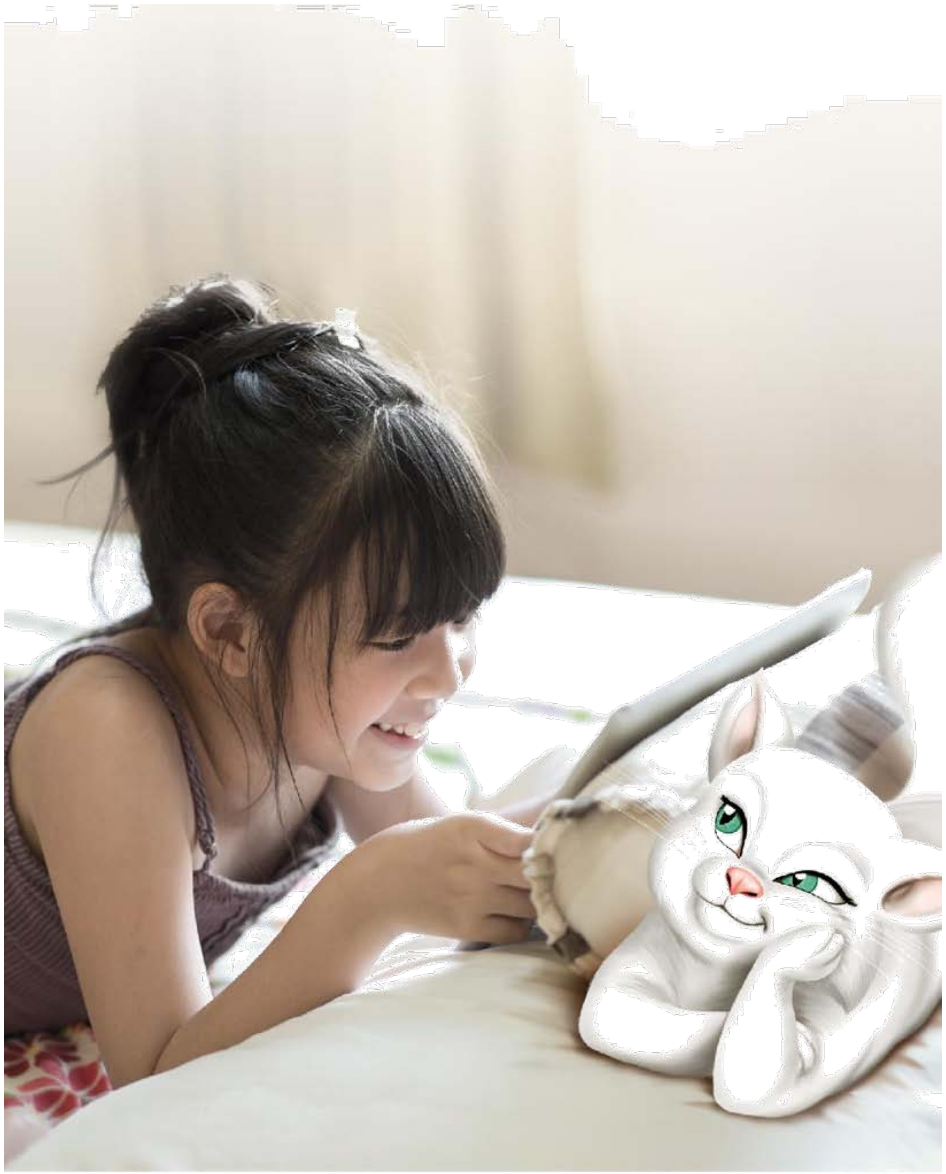
1: Çocuğunuza bir kullanıcı hesabı verin. Bu, çevrimiçi faaliyetlerini etkili bir şekilde kontrol etmek için ilk adımdır.
Sistem yöneticisi rolü her zaman bir yetişkine ait olmalıdır.

2: Antivirüs ve ebeveyn kontrol araçlarınızı güncel tutun.

3: Çocuğunuzun tarama geçmişini denetleyin. Eğer geçmiş silinmişse bu, bir konuşma yapmak için iyi bir nedendir.

4: Web kamerasını kontrol edin ve kullanımda olmadığı zamanlarda bağlantısının kesik ve (eğer yerleşikse) üstünün kapalı olduğundan emin olun.

5: Çocuğun sosyal ağ ayarlarını kontrol edin. Her şeyin sınırsız olarak herkese açık şekilde paylaşıldığı bir profil, bir gencin manevi bütünlüğünü riske atabilir.



Sonuç

Günümüzde, çocuğunuzun teknolojilere erişimini yasaklamak bir çözüm değildir. Onlar çocuğunuzun günlük yaşamının bir parçasıdır ve gelişimleri için giderek daha önemli hale gelmektedir. Kısıtlamalar koymak yerine, çocuklarınızın bunları güvenle kullanmasına yardımcı olarak çocuk ve cihaz arasındaki etkileşimde yer alın. Ayrıca bu risklerin çoğunun yetişkinleri de etkileyebileceğine ve burada açıklanan önlemlerin çoğunun her durumda ve her yaşta alınması gerektiğine dikkatinizi çekmek istiyoruz.

Çocukların güvenliği herkesin sorumluluğundadır ve bu kılavuzda verilen ipuçları, yetişkinlerin çocuğun bilgilerini, sistemlerini ve manevi bütünlüğünü korumalarına yardımcı olacaktır. Daha fazlası için web sitemizi ve sosyal ağlarımızı ziyaret edin:

www.eset.com.tr
www.welivesecurity.com

Sayfamızı Beğenin www.facebook.com/ESETTurkiye
Bizi takip edin: https://twitter.com/ESETTurkiye