

SİBER RİSKLER VE ALINABİLECEK TEDBİRLER





Sevgili Ebeveynler;

Bebekliklerinden itibaren onlar için güvenli ortamlar
oluřturdunuz...



- İnternetin sayısız faydasını zarara dönüştürmeyin..
- Şiddetten özel hayatın ihlaline, dolandırıcılıktan uyuşturucuya, cinsel istismardan kumara..



Suçla ilişkili bir çok kişi internet yolu ile evinize girebilir.

- Özellikle çocuklarımız mağdur olabilir. Lütfen dikkatli ve koruyucu olun.



Güvenli internet bilinçli kullanımla olur!.



- Dijital dünyadaki risklerin neler olduğunu öğrenmek, uygun önlemler almanızı kolaylaştıracaktır.



BÖLÜM 1



İNTERNETTE NELER OLABİLİR?



Uygunsuz İeriklere Maruz Kalma

- ocuklarınız internette uygun olmayan bilgiler veya grntlerle karşılaşabilir.
- Bir e-posta ya da IM'deki (anlık mesajlaşma) bağlantıyı tıklayarak ya da web de gezinirken cinsel içerikli ya da nefret dolu uygunsuz içeriklerle karşılaşabilir.



İnternet Üzerinden Tehdit

- Arkadaş gibi görünen kötü insanlarla karşılaşabilir. Birçok insan çevrimiçinde interneti diğerlerini taciz etmek, küçük düşürmek veya tehdit etmek için kullanır.
- Saldırıları lakap takmaktan, fiziksel tehdide kadar değişebilir ve nadiren aileler tarafından görülür.



Bilgi paylaşımı

- İnsanlar farkında olmadan ya da bilerek çocukların bilgilerini açıklayabilir.
- Okul ya da kulüplerin web sitelerinde genelde öğrenciler ve üyeler hakkında çok fazla kişisel bilgi paylaşılır..



- Arkadaşları bloguna bıraktıkları yorumlarla veya bilgi içeren fotoğraflarla çocuğunuzu riske sokabilirler. Saygın olmayan işletmeler topladıkları bilgiyi satabilir.



Tehlikeli Kişilere Maruz Kalma

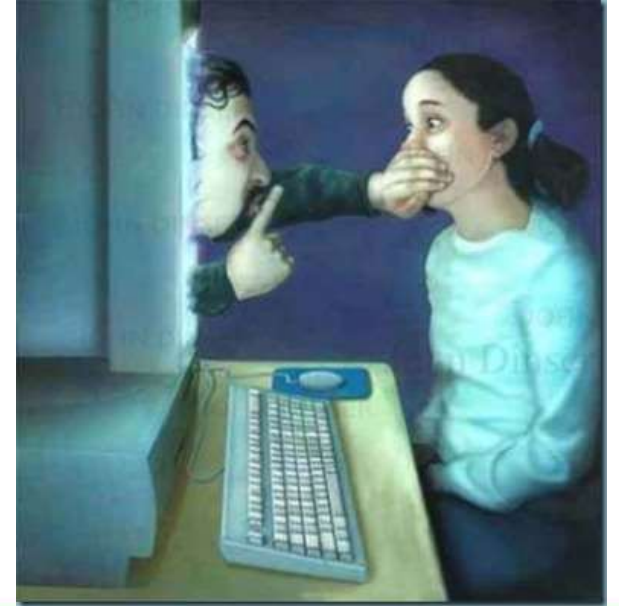


- Tacizciler bir çocuk veya güvenilir bir yetişkinmiş gibi davranarak veya çocukların macera arzularını kullanarak interneti korunmasız çocuklarla arkadaş olmak için kullanabilir ve daha sonra buluşmak için çocukları ikna edebilir.



Gizlilik İhlali ve Çevrimiçi Dolandırıcılık

- Çocuklar oyun oynarken veya kayıt formlarında kendileri veya aileleri hakkında fotoğraf veya kişisel bilgilerini ve şifrelerini paylaşabilir.
- Bu da tespit edilmelerini kolaylaştırır.
- Bu tür bilgiler, çocukların nefret saldırıları, kimlik hırsızlığı, dolandırıcılık veya çocuk tacizi gibi risklere karşı korunmasız kalmalarına neden olur.



Dosya paylaşımı dolandırıcılıkları

- Çevrimiçinde müzik, video ve diğer dosyaları almak risklidir.
- Bazı insanlar video ve müzik gibi görünen dosyalar paylaşır ancak bunlar aslında pornografik içerik olabilir ya da bilgisayarınızın saldırılara açık kalmasını sağlayan virüsler olabilir.



- Çocuklar bilgisayarınızda depolanan verilere zarar verebilecek, bunları silebilecek ya da kopyalayabilecek zararlı yazılımların yüklenmesine neden olabilir.

BÖLÜM 2



SİBER ZORBALIK !!!



Siber zorbalık nedir ?



Bir birey yada gurubun internet ve cep telefonu gibi bilgi ve iletişim teknolojilerini kullanarak kasıtlı ve sürekli olarak başkalarına zarar vermeye çalışmasıdır.



Çocukların Güvenliđi İçin Alınacak Önlemler

- Konu çocukların çevrimiçi güvenliđi olduđunda ebeveyn müdahalesi gözetimi ve rehberliđinin yerine geçebilecek bir teknoloji bulunmamaktadır.



- Çevrimiçi güvenlik, bir güç savaşı değil bir aile çalışmasıdır.



Çocuğumun siber zorbalığa maruz kaldığını nasıl anlarım?

- Çocuklar ve ergenler genellikle internet özgürlüklerinin ellerinden alınmasından çekindikleri , ebeveynlerinin vereceği tepkilerden korktukları veya yaşadığı zorbalıktan utandıkları için bu durumu saklamayı tercih ederler.
- Çocuklarındaki davranış değişikliklerini kontrol altında tutun; interneti kullanma konusunda isteksizlik veya doğal olmayan ağzı sıkılık problem olduğuna dair ipucu verebilir.



SİBER ZORBALIĞA MARUZ KALAN ÇOCUKLARDA NELER GÖRÜLEBİLİR

- Çocukta üzüntü, korku, öfke, aşağılanmışlık hissi, nefret, intikam isteği gibi duygular; okuldan kaçma, okula devamsızlık, kuralları çiğneme, saldırganlık gibi davranışlar ortaya çıkabilir.
- Çocuklarda depresyon, madde kullanımına suç işlemeye eğilim ve okul başarısının düşmesi de sanal zorbalığın psikolojik etkileridir.



NELER YAPABİLİRİM ?

- Çocuklarınızla, çevrimiçinde neleri sevdikleri ve görüştükleri arkadaşları hakkında sık sık konuşun.
- Kendilerini çevrim içinde rahatsız eden her şeyi, bilgisayar izinlerini kaybetme korkusu olmadan anlatabilecekleri bir ortam oluşturun.
- Eğlenceye katılın. Çocuğunuzla ve webdeki diğer arkadaşlarıyla beraber oyun oynayın. Ya da onlar oynarken yanlarında oturun.



NELER YAPABİLİRİM ?

- Bilgisayarları ve oyun aygıtlarını oturma odası gibi merkezi bir konuma yerleştirin. Çocuklarınızın çevrimiçindeyken neler yaptıklarını görün ve işitin.
- Çocuklarınızın çevrimiçinde hangi oyunları oynadığını ve hangi sohbet odalarını ziyaret ettiğini öğrenin.



NELER YAPABİLİRİM ?

- Çocuklarınızla, internet riskleri ve davranışlarının bu riskleri nasıl artırabileceği veya azaltabileceği hakkında konuşun.
- Çocuklarınızın öğretmen olmasına izin verin. Çocuklarınız en yeni siteler ve en son çevrimiçi trendleri size öğretebilir. Çocuklarınızı dünyalarını anlatmak konusunda teşvik etmek onlarla iletişim kurmak için harika bir yöntemdir



NELER YAPABİLİRİM ?

- Çocuklarınıza içgüdülerine güvenmeleri gerektiğini ve çevrimiçinde gerçekleşen bir olay nedeniyle tehdit edildiklerini hissetmeleri veya korkmaları halinde hemen size söylemeleri gerektiğini anlatın.
- Çocuklarınızdaki davranış değişikliklerini kontrol altında tutun; interneti kullanma konusunda isteksizlik veya doğal olmayan ağzı sıkılık problem olduğuna dair ipucu verebilir.
- Çocukların sadece siz evdeyken interneti kullanmalarına izin verin.



Bir Ebeveyn Olarak Kurallarınız açık ve kesin olsun...

- Çocuklarınızın ne zaman ve nasıl Interneti kullanabileceđi hakkında açık kurallar koyun ve bunları bilgisayarın yakınına yerleřtirin.
- Hangi bilgileri paylaşmaması gerektiđini, hangi sitelere girmemesi gerektiđini anlatın. Bu kuralların kontrol için deđil korumak için olduđunu güzelce anlatın.
- Sorumlulukla hareket etmesini öğretin.



Nasıl Kurallar Koymalıyım?

- Gizli arkadaşlık isteyen yetişkinlere “**hayır**” demeli ve iletişimi durdurmalılar.
- İnternette tanıştığı bir kişiyle kesinlikle buluşmamalı. Çocuklarınızın çevrimiçinde tanıştığı kişiler, söyledikleri kişi olmayabilir veya kötü niyetli olabilir.



Nasıl Kurallar Koymalıyım?

- Kendilerini savunmalılar. Çevrimiçinde birileri rahatsız ya da tehdit ederse yoksaymalılar ve iletişim kurmamalılar. Gerekirse, çocuklarınızın uygun Web sitesi yöneticileri, okul müdürleri veya diğer yetkililere rapor etmesine yardımcı olun.
- Kesinlikle e posta ekleri açmamalı, müzik paylaşmamalı veya e-posta veya anlık mesajlardaki bağlantıları tıklamamalıdır. Zararlı yazılımlar veya rahatsız edici içerikler yüklüyor olabilirler.



Nasıl Kurallar Koymalıyım?

- Başkalarına, kendilerine davranılmasını istedikleri gibi davranmalılar. Çevrimiçinde başkalarını tehdit etmek kırıcı ve kaba olabilir; diğer insanlara saygılı, nazik ve dürüst olmayı öğrenmeliler.
- Diğerlerinin mülklerine saygı göstermeliler. Müzik, oyun ve diğer telif haklı malzemelerin izinsiz kopyalanmasının yaşadışı olduğunu bilmeliler.



Nasıl Kurallar Koymalıyım?

- Çocuklarınıza, kendileri veya aileniz hakkında kişisel bilgileri izniniz olmadan ve tanımadıkları veya güvenmedikleri kişilerle kesinlikle paylaşmamaları gerektiğini öğretin.
- Çocuklarınızın e-posta, anlık mesajlaşma, web günlüğü ve sosyal ağ sitelerinde kimlerle bilgi paylaştığını öğrenin.
- Tahmin edilmesi zor şifreler seçmelerini sağlayın
- Şifrelerini arkadaşlarıyla paylaşmamaları gerektiğini anlatın.



Nasıl Kurallar Koymalıyım?

- Çocuklarınızın kişisel ve müstehcen olmayan bir ad veya eposta adresi seçmesine yardımcı olun.
- Kişisel bilgileri paylaşmamasını öğretin. Kişisel bilgiler sadece çocuğunuzun adı, yaşı, telefon numarası veya adresi gibi veriler değil ayrıca fotoğraflar ve hissettiklerini de içerebilir. Çocuk tacizcileri kırılğan (üzgün, yalnız veya öfkeli) çocukları arar ve bazen ilgisiz gibi görünen bilgileri kullanarak çocuğun yerini tespit edebilir.



Ebeveynler çocukları için tehlike riskini nasıl en aza indirgerler?

- Yeni işletim sistemlerine dahil edilmiş ebeveyn denetimi yazılımlarını veya ücretsiz indirebileceğiniz yazılımları kullanabilirsiniz.
- Ev İnternet Hattınız için Aile/Güvenli İnternet Paketi tercih edebilirsiniz.
- Sosyal ağ web sitelerindeki yaş sınırlarına uyun. Çoğu sosyal ağ sitesi kullanıcılarının 13 yaş veya üzerinde olmasını şart koşar. Çocuklarınız bu siteler için tavsiye edilen yaşın altında ise, bu siteleri kullanmalarına izin vermeyiniz.



Ebeveynler çocukları için tehlike riskini nasıl en aza indirgerler? (2)

- Küçük çocuklar sohbet odalarını kullanmamalıdır – tehlikeleri çok fazladır. Çocuklarınız büyüdükçe onları çocuklara yönelik iyi izlenen sohbet odalarına yönlendirin. Hatta 13 yaşın üzerindeki çocuklarınızı dahi izlenen sohbet odalarını kullanma yolunda teşvik ediniz.
- Çocuklarınızın sohbet odalarına katılmaları halinde, hangi sohbet odalarını ziyaret ettiklerini ve kimlerle konuştuklarını bildiğinizden emin olun. Ne tür konuşmaların gerçekleştiğini bizzat görmek için sohbet alanlarını kendiniz izleyiniz.



Ebeveynler çocukları için tehlike riskini nasıl en aza indirgerler? (3)

- İnternet bağlantısı olan bilgisayarı kesinlikle çocuğun yatak odasında değil, evin ortak alanlarından birinde bulundurunuz.
- Bilgisayar ekranı kolaylıkla görülebilir bir yerde olduğunda avcıların çocuğunuzla ilişki kurması çok daha zorlaşır. Bilgisayar evinizin ortak alanlarından birinde olduğunda dahi çevrimiçi olduklarında çocuğunuzla birlikte oturunuz.
- Eğer tüm önlemler başarısız olur da çocuklarınız bir çevrimiçi avcıyla tanışarlarsa, çocuklarınızı suçlamayın. Tüm sorumluluk daima suçlunundur. Çocuğunuzun bu kişiyle daha fazla iletişim kurmasını engellemek için kararlı şekilde eyleme geçiniz.



Ebeveynler çocukları için tehlike riskini nasıl en aza indirgerler? (4)

- Çocuklarınız küçükken kendi e-posta hesaplarından ziyade ailenin e-posta adresini paylaşmalıdırlar. Çocuklarınız büyüdükçe, İnternet Hizmet Sağlayıcınızdan (ISP) ayrı bir e-posta adresi ayarlamalarını isteyebilirsiniz ancak çocuklarınızın postaları yine sizin hesabınızda kalabilir.



Ebeveynler çocukları için tehlike riskini nasıl en aza indirgerler? (5)

- Çocuklarınıza yabancılardan gelen anlık iletilere veya e-postalara asla yanıt vermemelerini söyleyin. Çocuklarınız halk kütüphanesi, okul veya arkadaşlarının evleri gibi denetiminiz dışındaki yerlerde bilgisayar kullanıyorlarsa, hangi bilgisayar korumalarının kullanıldığını öğrenin.



Çocuklarınız kurban olma risklerini azaltmak için ne yapabilirler?

- Asla bilinmeyen bir kaynaktan resim indirmemek – cinsel olarak açık olabilirler.
- E-posta filtrelerinden edinin.
- Çevrimiçiyken kendilerini rahatsız eden veya korkutan herhangi bir şey olduğunda bunu derhal bir yetişkine söylemek.
- Cinsel olarak kışkırtıcı kelimeler içermeyen veya kişisel bilgileri açığa vurmuyan, cinsiyet belli etmeyen bir ekran adı seçmek.



Çocuklarınız kurban olma risklerini azaltmak için ne yapabilirler? (2)

- Çevrimiçi kimseye kendileri hakkında (yaş ve cinsiyet dahil) veya aileleri hakkında kişisel bilgi vermemek ve çevrimiçi kişisel profilleri doldurmamak.
- Herhangi bir kimsenin çok kişisel veya cinsel olarak kışkırtıcı sorular sormaya başlaması halinde her tür e-posta iletişimini, anlık ileti sohbetlerini veya sohbetleri kesmek.
- İnternette gizliliklerini korumalarını hatırlatmak için bilgisayarın yanına aile çevrimiçi anlaşmasını asmak.



Çocuđunuz hedef alınırsa ne yapabilirsiniz?

- Çocuđunuzun çevrimiçi yazıřtıđı birinden cinsel olarak açık fotođraflar alması, e-posta veya çevrimiçi başka bir yolla kendisinden cinsel istekte bulunulması halinde derhal yerel polisinize başvurun. E-posta adresleri, web sitesi adresleri ve sohbet g¼nl¼kleri dahil t¼m bilgileri polisle paylaşmak üzere kaydedin.



GÜVENLİ İNTERNET EDİNİN!!!

- Güvenli internet, bütün internet abonelerine internet servis sağlayıcı şirketler tarafından ücretsiz olarak sunulan ve internetteki muhtemel zararlı içeriklerden sizi ve ailenizi koruyan alternatif internet erişim hizmetidir. Kolaydır ve bilgisayarınıza program kurmanıza gerek yoktur.
- Size Çocuk Profili ve Aile Profili olmak üzere iki seçenek sunar. İstedığınız zaman Güvenli İnternet hizmetini alabilir, istediğiniz zaman profilinizi değiştirebilir, isterseniz bu hizmetten vazgeçebilirsiniz.

