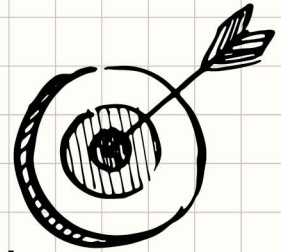




SİBER SUÇ VE SİBER ZORBALIKTAN



KORUNMA REHBERİ





İÇİN DE Kİ LER

SİBER SUÇ NEDİR?	6
SİBER SUÇLAR NELERDİR?	8
SİBER SUÇLARA KARŞI BAŞVURULACAK KURUMLAR VE İHBAR MEKANİZMALARI	10
SİBER SUÇLARDAN KORUNMAK İÇİN ALINACAK ÖNLEMLER NELERDİR?	12
SİBER ZORBALIK NEDİR?	14
HANGİ DAVRANIŞLAR SİBER ZORBALIKTIR?	16
SİBER ZORBALIĞIN NEDENLERİ NELERDİR?	18
SİBER ZORBALIĞIN MAĞDURLAR ÜZERİNDEKİ ETKİLERİ NELERDİR?	20
ÇOCUĞUMUN SİBER ZORBALIĞA MARUZ KALDIĞINI NASIL ANLARIM?	22
ÇOCUĞUMU SİBER ZORBALIKTAN NASIL KORUYABİLİRİM?	24
ÇOCUĞUM SİBER ZORBALIĞA MARUZ KALYORSA NE YAPABİLİRİM?	28
ÇOCUĞUM SİBER ZORBALIK YAPIYORSA NE YAPABİLİRİM?	30
YARARLANILAN KAYNAKLAR	32



Editör
Ayşegül YILDIRIM KARA

Hazırlayan
Esra KÖMÜR

Katkı Verenler
Eda ŞİRNEVAİ
Merve TEMİZ NALBANT
Aylin AKÇAY AYDOĞAN
Merve Nur YAVUZ

Tasarım-Dizgi
Selcan YILMAZ

İletişim

T.C. Aile ve Sosyal Hizmetler Bakanlığı Eskişehir Yolu Söğütözü Mah. 2177. Sokak No: 10/A
Çankaya/ANKARA Tel: 0 (312) 705 50 00

www.aile.gov.tr

Tüm hakları saklıdır. Kaynak göstermek ve ticari gelir elde etmemek koşuluyla kullanılabilir.





SİBER SUÇ NEDİR?



Siber suçlar, bir bilişim sisteminin güvenliğini, içindeki verileri veya kullanıcılarını hedef alarak teknoloji aracılığıyla gerçekleştirilen yasa dışı eylemlerdir. Bu suçların, bilişim sistemleri olmadan işlenememeleri onları diğer suç türlerinden ayırır.

Bilgisayar ve internet temelli suçlar olarak da adlandırılabilen bu eylemler, izinsiz şekilde bir sisteme girilmesi ve hukuka aykırı işlemler yapılmasıyla tanımlanır. Siber suçlarda hedef, bir kişi, kişinin malvarlığı ya da doğrudan sistemin kendisi olabilir.

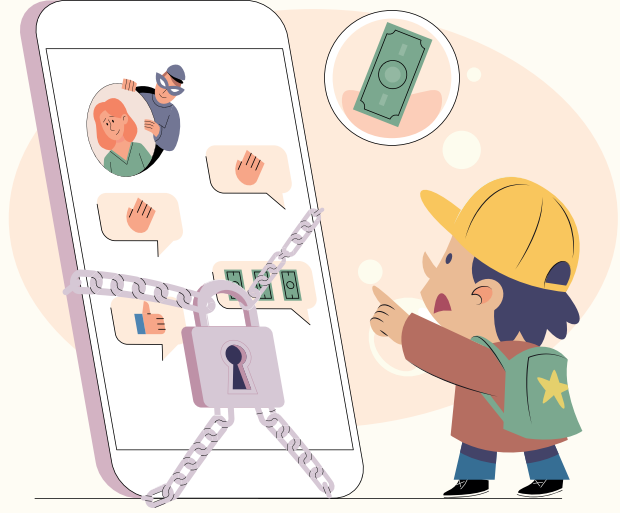




SİBER SUÇLAR NELERDİR?



- Ad, soyad, T.C. kimlik numarası, kredi kartı bilgileri gibi kişisel bilgilerin izinsiz olarak ele geçirilmesi, kaydedilmesi ve kötü amaçlarla kullanılması,
- Bir bilgisayar sistemine izinsiz olarak girilmesi, veri çalınması, veri eklenmesi, verilerin değiştirilmesi, bozulması, silinmesi veya başka bir yere gönderilmesi,
- Bir bilişim sisteminin işleyişinin engellenmesi, sisteme zarar verilmesi,
- Sahte e-postalar ya da sitelerle kullanıcıların bilgilerinin aldatma yoluyla ele geçirilerek kişisel verilerden menfaat sağlanması,
- Kişiler arasındaki haberleşmenin gizliliğinin ihlal edilmesi, iletişimin izinsiz olarak izlenmesi veya kaydedilmesi,
- Bir web sitesine veya sunucuya aynı anda çok sayıda istek göndererek sistemi çökertme amacıyla saldırı düzenlenmesi,
- Kişilerin özel hayatlarına dair bilgilerin izinsiz olarak elde edilmesi veya yayılması,
- Başkasına ait banka ve kredi kartı bilgilerinin ele geçirilmesi ve bu bilgilerin izinsiz kullanılması,
- Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretilmesi, satılması, devredilmesi, satın alınması veya kabul edilmesi,
- Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartının kullanılması,
- Çocukların istismarını içeren içeriklerin üretilmesi, dağıtılması veya paylaşılması,
- İnternet üzerinden yasa dışı kumar faaliyetleri yürütülmesi,
- İnternet aracılığıyla kişilere yönelik tehdit, aşağılama veya taciz eylemleri gerçekleştirilmesi,
- Bir cihazın, bilgisayar programının, şifrenin veya güvenlik kodunun bilişim sistemlerinin araç olarak kullanılması suretiyle, diğer suçların işlenmesi için yapılması veya oluşturulmasıdır.





SİBER SUÇLARA KARŞI BAŞVURULACAK KURUMLAR VE İHBAR MEKANİZMALARI



Suçla ilgili deliller
ile birlikte en
yakın Cumhuriyet
Başsavcılıklarına
veya Kolluk
Kuvvetlerine şahsen
müracaat edilebilir
ya da;



112 Acil Çağrı
Merkezi

<https://onlineislemler.egm.gov.tr>



CİMER (Cumhurbaşkanlığı İletişim
Merkezi) aracılığıyla
ihbarda bulunulabilir.

Bilgi Teknolojileri ve İletişim Kurumu (BTK) bünyesinde faaliyet gösteren Ulusal Siber Olaylara Müdahale Merkezi (USOM) tarafından zararlı internet adresleri olduğu tespit edilen oltalama, zararlı yazılım yayan ve/veya barından, komuta kontrol merkezi adresleri, port taraması yapan internet adreslerinin erişim engellemeleri yapılarak siber tehditlerin, olayların etkilerinin azaltılması, ortadan kaldırılması sağlanır.

Bu çerçevede, USOM'un resmi internet sitesinde bulunan <https://www.usom.gov.tr/ihbar> adresi üzerinden ihbar kaydı oluşturulabilir.

USOM ihbar hattı (0312 586 5305 - 0549 779 8785) aranarak veya ihbar@usom.gov.tr e-posta adresi üzerinden vatandaşlar tarafından zararlı internet adreslerine ilişkin siber suçlara dair başvuruda bulunulabilir.



SİBER SUÇLARDAN KORUNMAK İÇİN ALINACAK ÖNLEMLER NELERDİR?



- Açık ve güvenliği şüpheli internet ağlarına bağlanmaktan kaçının. Özellikle bankacılık işlemleri veya şifre gerektiren uygulamaları kullanırken bu ağlara bağlanmaktan kesinlikle uzak durun.
- Güvenli bir internet bağlantınız yoksa çevrim içi işlemlerinizi erteleyin.
- Toplu taşıma araçları, kafeler gibi yerlerde cihazınızı kullanırken ekranınızı başkalarının görmesini engelleyin. Özellikle şifrelerinizi veya hassas bilgilerinizi girerken bu konuya dikkat edin.
- İşletim sisteminizin, uygulamalarınızın ve antivirüs programınızın güncel olduğundan emin olun. Bu güncellemeler sizi olası tehditlere karşı korur.
- Önemli verilerinizi düzenli olarak yedekleyin.
- İnternette alışveriş yaparken sitenin güvenilir olduğundan emin olun. Sitenin güvenlik sertifikasının olması önemlidir. Ayrıca alışveriş yaptığınız web sitesinde 3D Secure seçeneği varsa, bu yöntemi kullanmanız güvenliğiniz için önemlidir.
- Tüm hesaplarınız için aynı parolayı kullanmayın. Her hesap için farklı ve güçlü parolalar oluşturun. Parolalarınızda büyük harf, küçük harf, sayı ve özel karakterler bulundurun.
- E-posta, SMS veya sosyal medya üzerinden gelen şüpheli linklere tıklamayın. Bilmediğiniz kişilerden gelen ekleri açmayın. Banka veya kredi kartı bilgilerinizi soran mesajlara itibar etmeyin.
- Hesaplarınız için iki faktörlü doğrulama özelliğini etkinleştirin.
- Kameranızı kullanmadığınızda kapalı konumda tutun.
- Telefonda kendisini polis, hâkim, savcı olarak tanıtır kişisel bilgilerinizi isteyen kişilere bilgilerinizi vermeyin.
- İnternette tanıştığınız kişilerle iletişim kurarken dikkatli olun. Onlara ad, soyad, adres gibi kişisel bilgilerinizi vermeyin.





SİBER ZORBALIK NEDİR?

Siber zorbalık; bir kişinin ya da grubun başka bir kişiye ya da gruba yönelik olarak, sosyal medya, e-posta, cep telefonu, internet ya da başka bir dijital araç kullanarak rahatsızlık ya da zarar vermek amacıyla yaptığı davranışlardır. Davranışın siber zorbalık sayılması için;

- Bilgisayar, internet, cep telefonu gibi dijital iletişim araçları kullanılarak yapılması,
- Davranışı yapan kişinin, karşıdakinin zarar göreceğinin farkında olması,
- Davranışın bir defalık olmaması, tekrarlayan şekilde devam etmesi gerekmektedir.

Bir defa yapılması, davranışın yanlış olmadığı anlamına gelmez, sadece tanımın ismi değişir. Tek seferde gerçekleşen davranış siber saldırı olarak tanımlanır.





HANGİ DAVRANIŞLAR SİBER ZORBALIKTIR?



- İnternet veya cep telefonu aracılığıyla başkalarına isim takmak, kişiyle alay etmek ya da kişiyi tehdit etmek,
- Bir kişinin özel hayatına dair bilgileri ifşa ederek mahremiyetini ihlal etmek,
- Kişinin paylaşılmasından hoşlanmayacağı görüntülerini izinsiz olarak paylaşmak,
- Kişinin rızası olmadan fotoğrafını veya videosunu yayınlamak,
- Bir kişiyle alakalı olarak karalayıcı, aşağılayıcı web sayfaları hazırlamak,
- Gerçek olmayan ve dedikodu niteliğinde bilgiler yayarak kişinin itibarını zedelemek,
- Çevrimiçi ortamlarda fiziksel veya psikolojik zarar verme tehdidinde bulunmak; olumsuz, aşağılayıcı ve alay edici mesajlar göndererek kişiyi rahatsız etmek,
- Başka birinin e-posta, sosyal medya veya oyun hesaplarına izinsiz girmek, şifrelerini değiştirmek ve bu hesaplar üzerinden uygunsuz içerikler paylaşmak veya zararlı eylemlerde bulunmak,
- Başka birinin adına sahte hesaplar açarak o kişinin adına olumsuz yorumlar yapmak, arkadaşlarını eklemek veya özel mesajlar göndermek,
- Bir kişinin sosyal ağlardaki tüm hesaplarını onu rahatsız edecek biçimde takibe almak, kişiyi takip ederek sürekli aynı yerlerde bulunarak rahatsızlık vermek,
- Kişiyi çevrimiçi ortamlardan (oyunlar, sosyal medya platformları gibi) kasıtlı olarak dışlamak, arkadaşlık isteklerini reddetmek veya gruplardan atmak,
- Ortak arkadaşları organize ederek hedef olarak seçilen bireyi arkadaş listelerinden silmelerini ve engellemelerini, yani sosyal olarak dışlamalarını sağlamak,
- Kişinin yaptığı paylaşımlara sürekli olumsuz, aşağılayıcı veya saldırgan yorumlar yapmak, vb. eylemler siber zorbalık davranışları arasında yer almaktadır.



SİBER ZORBALIĞIN NEDENLERİ NELERDİR?



Kişinin daha önceden siber zorbalık ile karşılaşmış ve bu durumdan zarar görmüş olması,

Özgüven eksikliği,

Düşük benlik algısı,

Empati eksikliği,

Düşük özsaygı,

Sosyal kaygı,

Aile içi huzursuzluklar,

Başkaları üzerinde güç kurma ve kontrol sağlama ihtiyacı,

siber zorbalığın nedenleri arasında yer almaktadır.





SİBER ZORBALIĞIN MAĞDURLAR ÜZERİNDEKİ ETKİLERİ NELERDİR?



- Siber zorbalığa maruz kalan bireyler olağan halinden farklı olarak; kızgınlık, endişe, üzüntü, stres, korku gibi olumsuz duygular yaşayabilirler.
- Arkadaşlık ilişkisi kurmada güçlük, arkadaşlık ilişkilerinde güvensizlik ve çatışma, içe kapanma, yalnızlık hissi ve sosyal izolasyon gibi sorunlar ortaya çıkabilir.
- Kişi kendini değersiz hissedebilir.
- Özsaygıda düşüş yaşanabilir.
- İştah ve uyku düzeninde değişim yaşanabilir.
- Derslere karşı ilgi kaybı, konsantrasyon güçlüğü ve uyku problemleri gibi durumlar ortaya çıkabilir ve bu durum akademik başarıyı olumsuz etkileyebilir.
- Okula gitmek istemeyebilir.
- Dijital cihazlardan bildirim aldığı anda gerginlik yaşayabilir.
- Yaşanan haksızlığı gidermek amacıyla zorbaya karşı benzer davranışlarda bulunma eğilimi görülebilir.
- Yaşananları kimseye anlatmama, utanç veya korku nedeniyle durumu görmezden gelme durumu olabilir.
- Bazı durumlarda, yaşanan siber zorbalığın etkisiyle fiziksel şiddete başvurma eğilimi görülebilir.





ÇOCUĞUMUN SİBER ZORBALIĞA MARUZ KALDIĞINI NASIL ANLARIM?

Çocuğunuzda;

- Aileden, arkadaşlardan ve sosyal etkinliklerden uzaklaşma eğilimi,
- Okul başarısında belirgin bir düşüş ve derslere olan ilgide azalma,
- Evde sürekli sinirli, kızgın ya da endişeli bir ruh hali içerisinde bulunma,
- Okul veya grup etkinliklerinden uzak durma ve bu ortamlardan kaçınma,
- Uyku düzeninde, beslenme alışkanlıklarında ve fiziksel sağlıkta önemli değişiklikler,
- Bilgisayar, telefon gibi elektronik cihazlardan uzaklaşma ya da bu cihazları kullanırken gerginlik yaşama,

- Mesaj veya e-posta gibi iletişim araçlarına gelen bildirimler karşısında aşırı tepki verme, aceleci ve gergin davranma, gibi durumlar gözlemleniyorsa, siber zorbalığa maruz kalma ihtimali göz önünde bulundurulmalıdır.





ÇOCUĞUMU SİBER ZORBALIKTAN NASIL KORUYABİLİRİM?



- Çocuğunuzla internet ve sosyal medya kullanımı hakkında açık ve samimi bir sohbet ortamı oluşturun. Onun yaşadığı sorunları dinleyin ve endişelerini anlamaya çalışın.
- Çocuğunuzun interneti güvenli bir şekilde kullanması için ona yol gösterin.
- Çevrimiçi arkadaşlıklar yerine çocuklarınızı gerçek hayatta sosyalleşmeye ve yüz yüze iletişim kurmaya teşvik edin.
- Güvenilir bilgi kaynaklarını kullanmaya teşvik edin
- Virüs ve casus yazılımları engelleyici programlar kullanın.
- Birlikte internet kullanımına dair kurallar belirleyin. Hangi sitelere girebileceği, ne kadar süre internette kalabileceği gibi konularda anlaşın.
- Çocuğunuzun internet kullanımını yakından takip edin. Bilgisayarlar ve akıllı cihazlar için Güvenli İnternet Hizmeti kapsamında sunulan Aile Profili/Çocuk Profilini kullanabilirsiniz.
- Güvenli parolalar oluşturmalarını ve bu parolaları başkalarıyla paylaşmaması gerektiğini öğretin.
- Kaynağına güvenmediği ya da tanımadığı kişilerden gelen iletileri açmaması gerektiğini öğretin.
- Yabancılardan gelen arkadaşlık isteklerini kabul etmemesi gerektiğini öğretin. Kişisel bilgilerini sosyal ağlarda/başkalarının erişimine açık ortamlarda paylaşmamasını sağlayın.
- İnternette içerik paylaşmadan önce düşünmesi gerektiğini öğretin.



- Sosyal medya hesaplarının gizlilik ayarlarını gözden geçirin. Sadece tanıdık kişilerin profilini görebilmesini sağlayın.
- Çocuğunuzun size her zaman güvenebileceğini hissettirin. Siber zorbalığa maruz kaldığında çekinmeden size, öğretmenine veya güvendiği bir yetişkine başvurabileceğini belirtin.
- Dijital dünyada da haklarımız olduğu ve bu hakları savunabileceğimiz konusunda çocuğunuzun bilgilendirin.
- Kendi haklarımızı savunurken aynı zamanda başkalarının haklarına saygı duyulması, başkalarını rahatsız edecek türdeki paylaşımların yapılmaması ve birisi hakkında paylaşım yapılmadan önce izin alınması gerektiğini öğretin.
- Siz de çocuğunuz için iyi bir örnek olun. İnterneti saygılı ve sorumlu bir şekilde kullanın.



Unutmayın, siber zorbalıkla mücadele hepimizin görevidir. Çocuklarımızı bu konuda bilinçlendirerek ve onlara destek olarak daha güvenli bir dijital dünya oluşturabiliriz.





ÇOCUĞUM SİBER ZORBALIĞA MARUZ KALİYORSA NE YAPABİLİRİM?

- Çocuğunuzun o anki güvenliğinden emin olun ve tehlikenin devam edip etmediğini kontrol edin. Çocuğunuzun açıkça ve rahatlıkla konuşabileceği, kendisini güvende hissedeceği bir ortam oluşturun.
- Çocuğunuzla konuşurken sakın olmaya özen gösterin. Panik yapmak, çocuğunuzun endişelenmesine veya size açılmaktan çekinmesine neden olabilir. Ona karşı olumlu bir tavır sergileyerek rahatlmasını sağlayın.
- Çocuğunuzun yargılamadan dinleyin, ona güvendiğinizi gösterin ve çocuğunuzun duygularını anlamaya çalışın.
- Çocuğunuzun siber zorbalık yaşaması durumunda öfke veya suçlama gibi tepkiler vermek yerine, sorunu çözmeye odaklanın ve çözüm için adımlar atın.
- Çocuğunuzun hangi platformlarda, kimler tarafından ve ne tür mesajlarla karşılaştığını öğrenmeye çalışın.
- Çocuğunuza siber zorbalık karşısında karşılık vermemesi gerektiğini bildirin.
- Zorbalık içeren mesajlar, yorumlar veya paylaşımların ekran görüntülerini alın. Bu, ileride gerekirse kanıt olarak kullanabileceğiniz bilgiler sağlar.
- Çevrim içi platformlarda ilgili platformun şikâyet mekanizmalarını kullanın. Durumu yetkililere bildirmek, sorunun çözülmesi için önemli bir adımdır.
- Eğer çocuğunuz okuldan biri tarafından siber zorbalığa uğruyorsa, durumu okul yönetimi veya öğretmenlerle paylaşın.
- Zorbalık yapan kişiyi zorbalık yaptığı platformdan engelleyin.
- Çocuğunuzun yanında olduğunuzu ve onu koruyacağınızı hissettirin, kendini güvende hissetmesini sağlayın.
- Çocuğunuzun bir daha aynı duruma maruz kaldığında size ya da öğretmenine durumu anlatmasını teşvik edin.
- Çocuğunuzun internet kullanımıyla ilgili güvenlik ayarlarını ve izinleri gözden geçirin. Gerekirse gizliliği artırmak için yeni ayarlar yapın.
- Çocuğunuzun siber zorbalık yaşaması psikolojik etkiler doğurabilir. Gerekirse bir uzman ile görüşmesini sağlayarak destek almasına yardımcı olun.



ÇOCUĞUM SİBER ZORBALIK YAPIYORSA NE YAPABİLİRİM?

Çocuğun siber zorbalık yaptığı fark edildiğinde bu durumu görmezden gelmek yerine, çözüm odaklı bir yaklaşım benimsemek önemlidir. Çocuğunuzun bu davranışlarını değiştirmek için atabileceğiniz bazı adımlar yan sayfada yer almaktadır.



- Bir sorun olduğunu ve çocuğunuzun desteğe ihtiyacı olduğunu unutmayın.
- Sakin kalın ve çocuğunuzun suçlamadan, yargılamadan açık bir şekilde konuşmaya çalışın. Bu, çocuğunuzun size açılmasını ve yaşadığı durumu anlamasını kolaylaştırır.
- Çocuğunuzun neden böyle davrandığını anlamak için onu dikkatle dinleyin. Kendi perspektifinden olayları anlatmasına izin verin. Çocuğunuzun bu davranışı sergilemesinin altında yatan nedenleri anlamaya çalışın.
- Çocuğunuzun suçlamadan, davranışının yanlış olduğunu ve başkalarına zarar verdiğini net bir şekilde anlatın. Çocuğunuza siber zorbalığın sonuçlarını ve bu tür davranışların mağdurlar üzerinde yaratabileceği olumsuz etkileri açıklayın.
- Çocuğunuzun duygularını anlamaya çalışın. Belki kendisi de bir zorbalığa maruz kalmış olabilir veya başka bir sorun yaşıyor olabilir.
- Çocuğunuzun dijital aktivitelerini yakından takip edin ve gerektiğinde sınırlar koyun.
- Çocuğunuza yaptığı davranışların sorumluluğunu alması gerektiğini öğretin. Zorbalık yaptığı kişiden özür dilemesi ve hatalarını telafi etmek için adımlar atması gerektiğini anlatın.
- Çocuğunuzla birlikte bu tür davranışları tekrarlamaması için stratejiler geliştirin. Çocuğunuza olumlu ve saygılı dijital davranışları öğretin. İnternette nasıl güvenli ve olumlu bir şekilde etkileşimde bulunabileceğini anlatın.
- Çocuğunuzun boş zamanlarını değerlendirebileceği spor, sanat veya gönüllülük gibi etkinliklere yönlendirin.
- Okulu ve öğretmeniyle iş birliği içerisinde olun.
- Eğer çocuğunuzun siber zorbalık yapma davranışları devam ederse veya bu konuda zorlanıyorsanız uzmandan yardım almayı düşünün.
- Aile içinde sağlıklı iletişim ve destekleyici bir ortam oluşturun. Çocuğunuzun duygusal ihtiyaçlarını anlamaya çalışın ve onunla açık iletişim kanalları oluşturun.



YARARLANILAN KAYNAKLAR

Bilgi Teknolojileri ve İletişim Kurumu İnternet Yardım. Gençler ve çocuklar siber zorbalığa maruz kalmamak için neler yapabilir? <https://www.internetyardim.org.tr/siber-zorbalik/gencler-vecocuklar-siber-zorbaliga-maruz-kalmamak-icin-neler-yapabilir> adresinden alındı.

Kavurucu, Ö., & Küçük, L. (2021). Çağın Gelişen Sorunu Siber Zorbalık:. Medical Research Reports, 4(3), 50-56. SİBERAY.

Siber Zorbalık: <https://www.siberay.com/siber-zorbalik> adresinden alındı.

SİBERAY. Siber Suçlar: <https://www.siberay.com/siber-suclar> adresinden alındı.

TRT Çocuk Ebeveyn Akademisi. (2024, Ocak 25). Siber Zorbalık ve Korunma Önerileri: <https://ebeveynakademisi.trtcocuk.net.tr/makale/siber-zorbalik-ve-korunma-onerileri-16778892> adresinden alındı.

Unicef. Siber zorbalık: Nedir ve nasıl önlenir: <https://www.unicef.org/turkiye/siber-zorbal%C4%B1knedir-ve-nas%C4%B1l-%C3%B6nlenir> adresinden alındı.

YEŞİLAY. (2022, Ocak). Fizikselden Sanala Yeni Bir Şiddet Türü: Siber Zorbalık: <https://www.yesilay.org.tr/tr/makaleler>

