Siber Zorbalık

Siber zorbalık, dijital teknolojiler kullanılarak gerçekleştirilen zorbalıktır. Bu tür zorbalıklar sosyal medyada, mesajlaşma platformlarında, oyun platformlarında ve cep telefonlarında görülebilir. Hedef seçilen kişileri korkutmaya, kızdırmaya ya da utandırmaya yönelik olarak tekrarlanan bir davranıştır.

Siber Zorbalık Davranışları

- Sosyal ağlar ya da sohbet odaları gibi çevrimiçi ortamlarda başkalarına aşağılayıcı, alay edici, öfke dolu, kaba, cinsel taciz veya şiddet içeren mesajlar göndermek.
- Bir kişinin kişisel bilgilerini izni ve haberi olmadan internet ortamında paylaşmak.
- Sosyal ağlarda birisi hakkında dedikodu yaymak ya da özel hayatıyla ilgili konuları herkesle paylaşmak.
- Bir kişiye alakalı olarak karalayıcı, aşağılayıcı web sayfaları hazırlamak.
- Başkası adına sahte hesap açıp, onun kimliğine bürünmek. Bir kişinin sosyal ağlardaki tüm hesaplarını onu rahatsız edecek biçimde takibe almak.
- Sosyal ağlardaki paylaşımlarına sürekli olumsuz yorumlar yapmak.
- Ortak arkadaşları organize ederek hedef olarak seçilen bireyi arkadaş listelerinden silmelerini ve engellemelerini, yani sosyal olarak dışlamalarını sağlamak.

Siber Zorbalığa Karşı ne Yapabilirim ?

Cevap Verme
Birisi size siber zorbalık yapıyorsa, yanıt yapmayın. Bu gibi durumlarda yanıt vermek durumun daha da kötü bir hal almasına sebep olabilir.

Ekran Görüntüsü Al
Zorbalık olabileceğini düşündüğünüz herhangi bir mesajın, paylaşımın, gönderinin ekran görüntüsünü alarak durumu kayıt altına alın.

Engelle ve Bildir
Çoğu çevrimiçi platform bu özelliğe sahiptir, eğer biri sizi rahatsız ederse, o kişiyi engellediğinizden ve kullanılan sosyal medyaya platformuna bildirdiğinizden emin olun.

Büyüklere Bilgi Ver
Siber zorbalık sizi birçok farklı şekilde etkileyebilir. Sakın yalnız olduğunu düşünme. Ebeveynlerinize ve öğretmenlerinize ne olduğunu bildirin, bu gibi durumları kesinlikle saklamayın.

Gizliliğini Koru
Sosyal medya gizlilik ayarlarınızı yüksek tutun, tanımadığınız kişilerle arkadaşlık yapmayın. Sokakta tanımadığımız insanlarla kurmadığınız bağı çevrimiçi durumdayken de kurmayın.

Farkında Ol
Siber dünyada tüm önleyici ve güvenlik önlemleriyle güncel kalın.

İnternette Güvende Olun

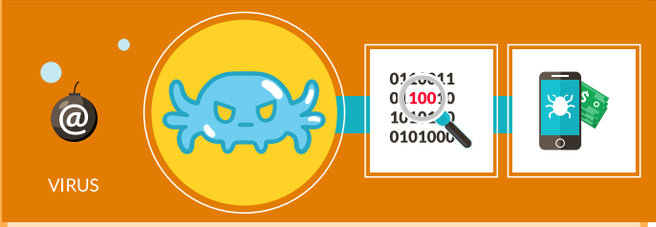
Molla Fenari Mah. Adem Yavuz Sok No 25 Nuruosmaniye
Fatih / İstanbul

Tel. : 0 212 522 94 06

www.buyukresitpasa.meb.k12.tr

BÜYÜK REŞİTPAŞA ORTAOKULU

GÜVENLİ İNTERNET KULLANIYORUZ



Bilgisayar Güvenliği

- Kullanmadığınız zamanlarda Bilgisayarınızın parolalı oturumunu kapatın ve gözetimsiz bırakmayın.
- Güç dalgalanmaları bilgisayara zarar verebileceğinden bilgisayarı doğrudan prize takmayın. Bunun yerine, bilgisayarı takmak güç kaynağı kullanın.
- Korsan yazılım yüklemeyin.
- Virüs içerebilecekleri için emin olmadığınız ve bilinmeyen cihazları bilgisayarınıza bağlamayın.
- Yalnızca doğrulanmış açık kaynak veya lisanslı yazılım ve işletim sistemlerini kullanın
- Kullandığınız anti virüs yazılımının düzenli olarak güncellendiğini kontrol edin.
- İçerik filtreleme yazılımı kullanarak .bat, .cmd, .exe, .pif gibi dosya uzantılara karşı dikkatli olun.
- Belirli güçlü parola yönergelerine sahip bir parola protokolüne sahip olun, parolalarınızı sık sık değiştirin, eski parolalarınızı yeniden kullanmamaya özen gösterin.
- Ağda kişisel USB'ler veya sabit sürücüler gibi kişisel cihazların kullanılmasını engelleyin.

İnternet Etiği ve Güvenliği

- Başkalarının mahremiyetine saygı gösterin
- Sohbet ederken, blog yazarken ve e-posta gönderirken dil kullanımında uygun protokolü izleyin.
- Başkalarının e-posta hesaplarına giriş yapmayın.
- Telif hakkıyla korunan materyalleri indirmeyin ve kullanmayın.
- Kötü amaçlı sitelerin tespit edilmesini sağlamak için otomatik tarayıcı güncellemesini etkinleştirin.

Güvenli E-mail

- Gerçek bir e-posta gibi görünse bile bilinmeyen gönderenden gelen e-postaları yanıtlamayın.
- İsim, doğum tarihi, okul adı, adres, ebeveyn isimleri gibi kişisel bilgileri veya diğer bilgileri vermeyin.

  Bilinmeyen bir kaynaktan geliyor olabileceği ve güvenilir olmayabileceği için kazançlı tekliflere / indirimlere kanmayın.
- Aygıtınızı etkileyebilecek kötü amaçlı dosyalar içerebileceğinden, bilinmeyen gönderenlerden gelen ekleri açmayın veya bağlantılara tıklamayın.
- Yalnızca güvendiğiniz web sitelerinden gelen bağlantıları ve indirmeleri tıklayın.
- Kimlik avı web sitelerine dikkat edin - web sitesinin güvenli olup olmadığını onaylamak için URL'yi kontrol edin.
- Başkalarına spam veya şüpheli e-postalar iletmeyin.

Güvenli Sosyal Medya

- Kimlik hırsızlığına yol açabileceğinden yaşınız, adresiniz, telefon numaranız, okulunuzun adı vb. Gibi kişisel bilgilerinizi çok fazla ifşa etmekten kaçının.
- Sosyal ağ sitelerinde gizlilik ayarlarınızı çok dikkatli yapın.
- Şifrenizi asla ebeveyniniz veya veliniz dışında kimseye açıklamayın.
- Yalnızca sizin tanıdığınız kişilerle iletişim kurun ve işbirliği yapın. Başkalarının duygularını incitecek hiçbir şey yayınlamayın.
- Sonsuza kadar çevrimiçi kalan dijital ayak izlerini bıraktıklarından, sosyal ağ sitelerinde fotoğraf, video ve diğer hassas bilgileri yayınlarken her zaman dikkatli olun.
- Arkadaşlarınızın bilgilerini ağ sitelerinde paylaşmayın, bu onları muhtemelen riske atabilir.
- Grup fotoğraflarını, okul adlarını, yerleri, yaşı vb. Yayınlamayarak arkadaşlarınızın mahremiyetini koruyun.
- Planlarınızı ve etkinliklerinizi ağ sitelerinde yayınlamaktan kaçının.
- Hiçbir sosyal ağ sitesinde kendiniz için sahte profiller oluşturmayın.
- Sosyal ağ hesap ayrıntılarınızın ele geçirildiğinden veya çalındığından şüpheleniyorsanız, hemen ağ oluşturma sitesinin destek ekibine bildirin.
- Sosyal medyada okuduğunuz hiçbir şeyi güvenilir bir kaynaktan doğrulamadan iletmeyin.
- Sosyal ağ siteleri aracılığıyla bağlantıları ve ekleri açmaktan her zaman kaçının.
- Giriş yaptıktan sonra hesabınızı asla gözetimsiz bırakmayın, kullanmadığınızda hemen çıkış yapın