GENEL E-GÜVENLİK KURALLARI

Daha güvenli ve daha emniyetli bir çevrimiçi deneyimi teşvik etmek için yaş veya mesleğe bakılmaksızın herkes için geçerli olan bazı e-güvenlik kuralları şunlardır:

Kişisel bilgilerinizi koruyun: Tam adınız, adresiniz, telefon numaranız, e-posta adresiniz ve finansal bilgileriniz dahil olmak üzere kişisel bilgilerinizi çevrimiçi olarak paylaşma konusunda dikkatli olun. Bu tür bilgileri yalnızca güvenli web sitelerinde ve güvenilir kişi veya kuruluşlarla paylaşın.

Güçlü şifreler kullanın: Her çevrimiçi hesap için benzersiz, karmaşık şifreler kullanın ve bunları düzenli olarak değiştirin. "123456" veya "şifre" gibi kolayca tahmin edilebilecek şifreler kullanmaktan kaçının. Güçlü parolaları güvenli bir şekilde oluşturmak ve saklamak için bir parola yöneticisi kullanmayı düşünün.

Kimlik avı girişimlerine karşı dikkatli olun: Kişisel veya mali bilgilerinizi isteyen veya sizi şüpheli bağlantılara tıklamaya veya ekleri indirmeye teşvik eden istenmeyen e-postalara, mesajlara veya aramalara karşı dikkatli olun. Yanıt vermeden veya herhangi bir işlem yapmadan önce gönderenin meşruiyetini doğrulayın.

Tıklamadan önce düşünün: Bağlantılara tıklarken, dosya indirirken veya bilinmeyen ya da güvenilmeyen kaynaklardan yazılım yüklerken dikkatli olun. Kötü amaçlı bağlantılar ve indirmeler, cihazınıza kötü amaçlı yazılım bulaştırabilir veya kimlik avı dolandırıcılıklarına yol açabilir.

İyi sosyal medya hijyeni uygulayın: Gönderilerinizi ve kişisel bilgilerinizi kimlerin görebileceğini kontrol etmek için sosyal medya platformlarındaki gizlilik ayarlarınızı gözden geçirin ve düzenleyin. Çevrimiçi olarak paylaştıklarınıza dikkat edin ve paylaşımda bulunmadan veya yorum yapmadan önce olası sonuçları göz önünde bulundurun.

Çevrimiçi ortamda saygılı ve düşünceli olun: Sosyal medya, mesajlaşma uygulamaları, çevrimiçi forumlar veya oyun platformları aracılığıyla çevrimiçi etkileşimlerinizde başkalarına saygılı ve nazik davranın. Siber zorbalık, taciz veya nefret söyleminden kaçının.

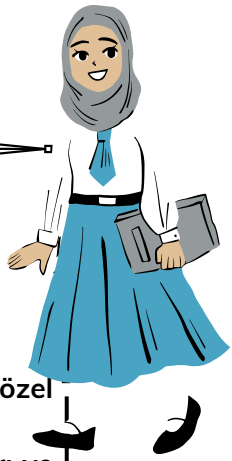
Bilgileri paylaşmadan önce doğrulayın: Çevrimiçi olarak karşılaştığınız bilgilere karşı eleştirel olun ve başkalarıyla paylaşmadan önce doğruluğunu saygın kaynaklardan doğrulayın. Yanlış bilgi ve sahte haberler hızla yayılabilir ve zararlı sonuçlar doğurabilir.

Cihazlarınızı ve verilerinizi koruyun: Bilgisayarlar, akıllı telefonlar ve tabletler de dahil olmak üzere cihazlarınızı en son güvenlik yamaları ve antivirüs yazılımlarıyla güncel tutun. Bir güvenlik ihlali veya cihaz arızası durumunda kaybı önlemek için önemli verilerinizi düzenli olarak güvenli bir konuma yedekleyin.

Çevrimiçi tehditler konusunda kendinizi eğitin: Kötü amaçlı yazılım, kimlik avı, kimlik hırsızlığı ve siber zorbalık gibi yaygın çevrimiçi tehditler hakkında bilgi sahibi olun. Kendinizi ve çevrimiçi ortamda başkalarını korumak için bu tehditleri nasıl tanıyacağınız ve bunlara nasıl yanıt vereceğiniz konusunda kendinizi eğitin.

İçgüdülerinize güvenin: Çevrimiçi ortamda şüpheli veya gerçek olamayacak kadar iyi bir şey geliyorsa, içgüdülerinize güvenin ve dikkatli davranın. Çevrimiçi ortamda herhangi bir şüpheli veya endişe verici davranışla karşılaşırsanız bunu ilgili yetkililere veya platform yöneticilerine bildirin.

Herkes bu e-güvenlik kurallarına uyarak kendisi ve başkaları için daha güvenli ve daha güvenli bir çevrimiçi ortam yaratılmasına katkıda bulunabilir.



ÖĞRENCİLERİN DİKKAT ETMESİ GEREKEN HUSUSLAR

Çevrimiçi deneyimlerinin güvenli ve olumlu olmasını sağlamak amacıyla öğrencilere özel olarak hazırlanmış bazı e-güvenlik kuralları şunlardır:

1.Kişisel bilgileri koruyun: Öğrenciler, tam adlar, adresler, telefon numaraları, okul adları ve diğer hassas ayrıntılar dahil olmak üzere kişisel bilgilerin çevrimiçi paylaşılması konusunda dikkatli olmalıdır. Bu bilgiler yabancılar tarafından zararlı amaçlarla kullanılabilir.

2.Güçlü parolalar kullanın: Öğrencilerin çevrimiçi hesapları için güçlü, benzersiz parolalar kullanmaya ve bunları asla kimseyle, hatta arkadaşlarıyla paylaşmamaya teşvik edin. Güvenliği artırmak için şifreler harf, sayı ve özel karakterlerin birleşiminden oluşmalıdır.

3.Göndermeden önce düşünün: Öğrencilerin, fotoğraflar, yorumlar ve mesajlar da dahil olmak üzere çevrimiçi yayınlayacakları şeyler hakkında dikkatli düşünmeleri gerekir. Bir şey çevrimiçi olarak paylaşıldığında onu silmek veya tamamen kaldırmak zor olabilir ve bunun gelecekte sonuçları olabilir.

4.Yabancılara karşı dikkatli olun: Öğrenciler, özellikle sohbet odalarında, sosyal medyada veya oyun platformlarında yabancılarla çevrimiçi etkileşime girme konusunda dikkatli olmalıdır. Onları, yalnızca internette tanıştıkları biriyle ebeveyn denetimi olmadan asla tanışmayı kabul etmemeleri konusunda teşvik edin.

5.Siber zorbalığı bildirin: Öğrenciler çevrimiçi ortamda siber zorbalığa, tacize veya başka uygunsuz davranışlara maruz kalır veya tanık olurlarsa, bunu derhal güvendikleri bir yetişkine bildirmelidirler. Okulların genellikle bu durumlarla başa çıkmak için protokolleri vardır.

6.Gizlilik ayarlarını belirleyin: Öğrencilerin sosyal medya platformları ve diğer çevrimiçi hesaplardaki gizlilik ayarlarının önemini anlamalarına yardımcı olun. Gönderilerini ve kişisel bilgilerini kimlerin görebileceğini kontrol etmek için onları gizlilik ayarlarını gözden geçirmeye ve düzenlemeye teşvik edin.

7.Çevrimiçi ortamda saygılı olun: Öğrenciler tüm çevrimiçi etkileşimlerinde başkalarına saygılı ve nazik davranmalıdır. Siber zorbalık ve çevrimiçi taciz ciddi sonuçlar doğurabilir ve asla hoş görülmemelidir.

8.Bilgileri doğrulayın: Öğrencilere çevrimiçi buldukları bilgileri eleştirel bir şekilde değerlendirmeyi ve bu bilgilere güvenmeden veya paylaşmadan önce doğruluğunu güvenilir kaynaklardan doğrulamayı öğretin. Yanlış bilgiler internette kolayca yayılır ve zararlı etkiler yaratabilir.

9.Ekran başında geçirilen süreyi sınırlayın: Öğrencileri çevrimiçi etkinliklerini egzersiz, hobiler ve arkadaşlarıyla ve aileleriyle vakit geçirmek gibi çevrimdışı etkinliklerle dengelemeye teşvik edin. Çok fazla ekran başında geçirilen zamanın fiziksel ve zihinsel sağlık üzerinde olumsuz etkileri olabilir.

Öğrenciler bu e-güvenlik kurallarına uyarak çevrimiçi dünyada daha güvenli ve sorumlu bir şekilde gezinebilir, riskleri en aza indirebilir ve teknolojinin faydalarını en üst düzeye çıkarabilir.