SIBER ZORBALIK

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.

AİLENE ANLAT!

Kötü ve sizi rahatsız eden mesajlara hiçbir zaman cevap vermeyin. Böyle bir mesaj almanız sizin suçunuz değildir. böyle bir mesaj alırsanız Anne ve babanıza veya güvendiğiniz Bir yetişkine söyleyin. onlarda Siber polise bildirsinler.

AİLENLE PAYLAŞ!

En sevdiğiniz web siteleri ve uygulamaların nasıl çalıştığını ailenize gösterin. onların İnternette neler yapılabileceğini anlamalarına yardımcı olun. Twitter ve Facebook gibi sosyal ağların kullanım kurallarına uyun.

PROF.DR. ŞABAN TEOMAN DURALI BİLİM VE SANAT MERKEZİ
2002
ZONGULDAK

KİŞİSEL BİLGİLERİNİ PAYLAŞMA!

Ev adresinizi, telefon numaranızı ve Okulunuzun ismi ve yeri gibi kişisel Bilgilerinizi internette paylaşmayın anne ve babanızın kişisel bilgilerini de internette kullanmayın.

Resimlerinizi kime gönderdiğinize dikkat edin. bazı kişiler bu resimleri sizlere zarar vermek için kullanabilirler

İNANMA!

Tanımadığınız veya güvenmediğiniz kişilerden gelen mesajlardaki ekleri açmayın; Bu mesajlar virüs içerebilir. bu virüsler Kişisel bilgilerinizin çalınmasına neden olur.

BİR BİLENE DANIŞ!

Program yüklerken anne babanıza veya öğretmeninize sorun. bazı programlar bilgisayarınıza veya ailenize zarar verebilir. internette her zaman dürüst olun.

SIBER ZORBALIK

Onaylama
Reddet
Korkma
Karşılık Verme
Misilleme Yapma

ANLAT!

E-GÜVENLIK

1- BASİT PAROLALAR

Parolanızı kırmak isteyen hackerlar Öncelikle herkesin kullandığı parolaları dener. şifre, isminiz, 1234 gibi tahmin edilmesi çok kolay olan parolalar sıkça kullanılıyor.

2- SOSYAL AĞ YÖNTEMLERİ

Eğer bir yöntem işe yaramadıysa Bu sefer de size sosyal ağ web sayfamızdan gelmiş gibi parolanızı girmeniz gerektiğini söyleyen sahte bir e-posta gönderebilir ve şifrenizi girmeniz istenebilir.

3- ŞİFRESİZ Wİ-Fİ AĞLAR

Şifresiz açık wi-fi ağları büyük bir güvenlik riski oluşturabilir. bu ağlardan gönderilen veriler wi-fi sinyalinin alınabildiği her yerden izlenebilir. buna SSL üzerinden gönderilemeyen parolalar da dahildir

4- VİRÜS VE PROGRAMLAR!

Zararlı programlar ile bilgisayarınızdaki tüm işlemler ve girilen şifreler hırsızlar tarafından izlenebilir. bilgisayarınızın ikinci bir sahibi gibi bilgisayarınızı istedikleri gibi kullanabilirler. Tüm şifre ve hesaplarınızı ele geçirebilirler. Öncelikle güncel antivirüs kullanın. Güvenli şifre seçin ve asla tanımadığınız kişilerden gelen şüpheli e-postaları açmayın.

4- E-POSTA'LARA DİKKAT!

Bazı casus yazılım veya virüsler e-posta yoluyla bilgisayarınıza ulaşabilir. Bundan dolayı tanımadığınız kişilerden gelen veya şüpheli görünen e-postaları açmayın.

Bilgisayarınıza bir e-mail ya da internetten indirdiğiniz film, müzik ve çoğu ücretsiz programların içinde olan bir virüs gizlenmiş olarak siz farkında olmadan bilgisayar, tablet ve mobil telefonlarınıza yüklenir. Kişisel bilgi ve şifreleriniz çalınmış olur.

5- SANAL KLAVYE KULLANIMI

Bilgisayarınıza key-logger bulaşmış olsa bile sanal klavye kullanımı hesabınızın ele geçirilmesi riskini azaltır.

SIBER GÜVENLIK

Güvenli Şifre
Güvenli Ağ
Güvenlik Yazılımı
Epostalara Güvenme

ANLAT!