Siber Saygı - Siber Zorbalık

- **Siber Zorbalık nedir?**

Siber: Canlı ile makine arası iletişim, sanal gerçeklik, sanal ortam demekse SİBER ZORBALIK ne demektir?

Siber zorbalık, "bilgi ve iletişim teknolojilerini kullanarak bir birey ya da gruba, özel ya da tüzel bir kişiliğe karşı yapılan teknik ya da ilişkisel tarzda zarar verme davranışlarının tümüdür.

İki çeşit siber zorbalık bulunmaktadır:

- elektronik zorbalık (daha çok teknik)
- elektronik iletişim zorbalığı (daha çok psikolojik)

1. Siber zorbalığa (sanal alem, internet zorbalığı) örnekler:
   - Kişilerin şifrelerini ele geçirmek
   - Web sitelerini heklemek
   - Spam içeren mailler göndermek ya da bulaşıcı mailler göndermek
   - Bilgi ve iletişim teknolojilerini kullanarak kişileri sürekli rahatsız etme
   - Kişilerle alay etme,isim takma
   - dedikodu yayma
   - internet üzerinden kişiye hakaret etme
   - kişinin rızası olmadan fotoğraflarını yayınlama
2. Siber zorbalık ile karşılaştığımızda neler yapmalıyız?
   1. En yakınımızdaki güvendiğimiz bir kişiye durumu haber vermeliyiz.
   2. 155 Polis İmdat hattını arayarak veya 155@egm.gov.tr' ye e-posta göndererek, "Bilişim Suçları ve Sistemleri Şube Müdürlüğü bildirimde bulunmalıyız.
   3. Cumhuriyet Savcılığı´na dilekçe ile durumu bildirmeli ve dava açmalıyız.
   4. Mahkeme, ISS (İnternet Servis Sağlayıcı) dan (Superonline, Turk Telekom gibi) suçlunun **IP** adresini ister.
   5. 5651 sayılı Bilişim Suçları Kanunu'na göre suçlunun cezası verilir.
3. Bilişim Suçları İle İlgili Alabileceğiniz Önlemler

✓ Şirketinize veya şahsınıza ait önemli bilgilerinizin yer aldığı bilgisayarınız ile özel güvenlik önlemleri almadan internete bağlanmayınız.
(Antivirüs programı kurmak, güvenlik duvarını açmak, filtreleme programı kullanmak, reklamları tıklamamak, sosyal medya hesaplarımızdaki profilleri herkese açık yapmamak (sadece arkadaşlarım görebilir yapmak), internette tanımadığımız kişilerle konuşmamak, kişisel bilgilerimizi paylaşmama.. vs)

✓ İnternet ortamında %100 güvenlik hiç bir zaman mümkün değildir. Özellikle sohbet (chat vb.) ortamında bilgisayarınıza saldırılabilir.

✓ Sohbet (chat vb.) ortamında tanıştığınız kişilere şahsınız, aileniz, adresiniz, telefonunuz, okulunuz v.b. konularda bilgi vermeyiniz. Tanımadığınız kişilerle konuşmayınız. Eğer tanımadığınız kişi sizi hesabına eklerse onu engelleyiniz. Yüz yüze tanımadıklarınızı siz de hesabınıza eklemeyiniz.

✓ İnternet ortamında tanıştığınız kişilere kredi kartı bilgilerinizi vermeyiniz.

- Eğer birisi size karşı saygısızca davranıyorsa o kişiyi engellenmiş kişiler listesine ekleyerek onunla tartışmalara girmemelisiniz. Eğer böyle bir kişi ile tartışmaya girerseniz bu davranışınızın onun daha çok hoşuna gideceğini bilmelisiniz.
- Koyu, kalın veya büyük harflerle yazı tipini bütün cümlelerde kullanmamalısınız. Çünkü büyük harf ya da koyu ve kalın yazı yazmak, dikkat çekmek, ya da kızgınlık anlamına gelmektedir.
- İnternetteki Takma Adınızı kötü söz içerecek şekilde kullanmamalısınız. Takma ad olarak tartışma yaratan isimler seçmeden, ahlaka uygun isimler seçiniz.
- Sohbet esnasında başkalarını rahatsız edecek şekilde ırk, din, dil, siyaset gibi konular hakkında açıklamalarda bulunmamalı ve diğerlerini de bu yolla rencide etmemelisiniz.
- Kanuna, ahlâka ve kamu düzenine aykırı mesaj içeriği göndermek, uygunsuz, yalan ve/veya iftira içerik ya da mesaj ve bilgileri göndermek, tehdit etmek, küfür, vb. fiilleri işlemek, kişi ve/veya kuruluşların gizli bilgilerini yayınlamak, reklam ve internet sitesi tanıtımını yapmak doğru bir davranış değildir.
- Eğer ilk defa bir sohbet kanalına girmiş iseniz, sohbete katılmadan önce orada olup bitenleri takip etmelisiniz. Eğer odadaki sohbet hoşunuza gitmediyse o sohbet odasını terk edebilirsiniz.
- Unutmayın ki; sohbette tamamen tanınmaz durumda değilsiniz. Tüm sohbet sunucuları giriş bilgileriniz üzerinden IP adresinizi (bilgisayarınızın numarası) ve hangi ISS (internet servis sağlayıcı) üzerinden internete girdiğinizi tespit edebilir. ISS de ise sizin ile ilgili bir çok bilgiler bulunmaktadır. IP adresiniz tespit edilebileceği için bilgisayarınızı başkalarının kullanması durumunda sorumluluğun size ait olduğunu unutmayınız.

- **Virüsler ve önlemleri**

Bilgisayar virüsü kullanıcının izni ya da bilgisi dahilinde olmadan bilgisayarın çalışma şeklini değiştiren ve kendini diğer dosyaların içerisinde gizlemeye çalışan aslında bir tür kötü bilgisayar programıdır.

Kötü amaçlı yazılım nedir?

Bilgisayar sistemlerine zarar vermek, bilgi çalmak, kullanıcıları rahatsız etmek gibi amaçlarla hazırlanmış yazılımlara genel olarak verilen ad. Kötücül yazılımlar, birçok farklı dosya türü içinde taşınabilmektedirler. Bu yazılımlar bulaştığı bir bilgisayar sisteminde veya ağ üzerindeki diğer makinelerde zarara yol açmak veya çalışmalarını aksatmak amacıyla hazırlanmış yazılımların genel adıdır.

Güvenlik Duvarı: Güvenlik duvarı, internet üzerinden sizin bilginiz ve isteğiniz dışında bilgisayarınıza erişilmesini engellemek üzere kullanılan bir yazılım ya da donanım olabilir.

Güvenlik Duvarı Nasıl Çalışır?: Güvenlik duvarı temel olarak bilgisayarınızın "kapısında" oturan bir güvenlik görevlisine benzer. Kimlerin ya da hangi yazılımların bilgisayarınıza giriş yapabileceklerini sıkı sıkı denetler. Güvenlik duvarları genellikle başlangıçta bilgisayarınızın internet bağlantısı da dahil bütün giriş çıkışı engeller, siz yazılımları kullandıkça size hangi yazılımlara ne kadar erişim hakkı vereceğini sorar.

Unutulmamalıdır ki, güvenlik duvarı hiçbir zaman yüzde yüz güvenlik sağlamaz. Güncellenmemi. Ve *güvenlik açıkları olan işletim sistemleri, zayıflıkları giderilmemiş programlar* ve *zayıf parolalara sahip kullanıcı hesapları*, güvenlik duvarının arkasında olsa bile güvende sayılmaz.

- **Virüslerden korunmak için :**
  - ✓ Antivirüs programları kurulmalıdır.
  - ✓ Güvenlik Duvarı programı açık olmalıdır.
  - ✓ Bu programlar güncellenmeli ve güncel tutulmalıdır.
  - ✓ İnternetten her dosya indirilmemelidir. İnternetten indirilen dosyalar virüs taramasından geçirilip temiz olduğu anlaşıldıktan sonra kullanılmalıdır.
  - ✓ Reklamlar tıklanmamalıdır.
- **Güvenli şifreler**
  - ✓ Şifremizde mutlaka büyük harf, küçük harf, sayı ve simge olmalı ve şifremiz uzun olmalıdır.
  - ✓ Başkaları tarafından kolay bulunabilecek şifreler seçilmemelidir.
  - ✓ Aynı harften ve sayıdan oluşan şifreler seçilmemelidir.
  - ✓ Ardışık sayılardan ve alfabe sırasından oluşan şifreler seçilmemelidir.
  - ✓ Şifre sahibinin gerçek hayatta kullandığı, şahsına ait özel numaraların tamamı veya bir bölümü şifre olarak seçilmemelidir.
  - ✓ Yer isimleri şifre olarak seçilmemelidir.
  - ✓ Klavyedeki harf düzeninden oluşan kelimeler şifre olarak seçilmemelidir.

✓ Dijital Ölçüler

- ✓ Bilgisayarda dosyalarımızı Sabit Disk, Flash Bellek, CD, DVD gibi depolama birimlerine kayıt ederiz ve bunların belirli büyüklükleri vardır. Örnek: 250 GB lık sabit disk, 8 GB lık flash bellek, 4 GB lık DVD, 700 MB lık CD gibi.
- ✓

✓ Dijital ölçü birimlerini sıralanışı:
✓ Bit - Byte - KiloByte - MegaByte - GigaByte – TeraByte

- ✓ Dijital Ölçü Birimlerini Birbirine Çevirme:
- ✓ 1 Byte = 8 bit
- ✓ 1 Kb (kilobyte) : 1024 byte'tan oluşur,
- ✓ 1 Mb (Megabyte): 1024 kb tan oluşur,
- ✓ 1 Gb (Gigabyte): 1024 Mb tan oluşur,
- ✓
- ✓ 1 Tb (Terabyte): 1024 Gb tan oluşur.
- ✓ Örnek Çözümlü Sorular:
- ✓ 1 KB kaç Bit'tir?
- ✓ 1 KB = 1024 Byte içerir 1 Byte = 8 Bit ise
- ✓ →1 KB = 1024 x 8 Bit
- ✓ 2048 MB kaç GB'tır?
- ✓ 2048 MB = 2048/1024=2 GB tır