

GÜVENLİ VE BİLİNÇLİ İNTERNET KULLANIMI

11-A Damla Kanođlu,Ömer Yıldırım



Gerçek Hayatta
İyilikler ve Kötülükler
Olduğu Gibi
İnternetin de
İyilikleri ve Kötülükleri
Vardır!!!

- Hayatın neredeyse her alanında evimizde, cebimizde, kafelerde, restoranlarda, AVM'lerde ve aklınıza gelebilecek her türlü ortamda interneti özgürce kullanabiliyoruz. Bu denli büyüyen ve gün geçtikçe gelişmeyi sürdüren internetin, gerek sosyal gerekse iş hayatındaki olumlu katkıları yadsınamaz ancak kimi zaman da pek çok olumsuz durumla da bizi yüz yüze bırakabiliyor. İşte bu noktada olumsuz durumları yaşamamak ya da en azından minimuma indirmek adına birtakım önlemler almak gerekiyor. Peki güvenli internet kullanımını için yapılması gerekenler neler?

Kişisel Bilgilerinizi Paylaşmayın

- Ev adresiniz, telefon numaranız gibi şahsi bilgileri paylaşmak için internet pek güvenli bir ortam değil. Şahsi bilgilerinizi tanımadığınız milyonlarca yabancı kişiye kendi ellerinizle teslim etmeyin.

Saygılı Davranınız

- Sanal ortamda size nasıl davranılmasını istiyorsanız sizde öyle davranın, yani saygılı. Kısacası sosyal medyayı ve interneti siber zorbalık yapıp, hakaret ederek kimseyi incitmek için değil, faydalı şeyler için kullanınız.

Kötü Mesajları Bildiriniz

- Sizi rahatsız eden, tehdit eden, dalga geçen ya da kendinizi kötü hissettiren bir mesaj aldığınız vakit bunu ilk olarak ailenize bildiriniz. Bu mesajları almanız sizin suçunuz değil. Daha sonrasında bu durumu daha üst yerlere bildirebilirsiniz.

Gördüğünüz Her Linke Ve Siteye Tıklamayınız

- İnternet ortamında karşımıza çıkan her link güvenli değildir. Siber suçlular, tehlikeli gibi gözükmeyen ancak içerisinde bir çok tuzak barındıran sahte içerikleri birer yem olarak kullanırlar. Siber suçlular bir çok insanın arama yaptıkları esnada buldukları kaynaklar şüpheli dahi olsa merak duygularına yenik düşeceklerini ve içeriklerin cazibelerine kapılıp gardlarını indireceklerini biliyorlar. Bu tarz dikkatsiz tıklamalar sonucunda kişisel verilerinizin açığa çıkabileceği gibi elektronik cihazlarınıza malware diye tabir edilen kötü amaçlı yazılımların yüklenmesine de sebebiyet verebilir.

Ne İndirdiðinize Dikkat Ediniz

- Siber suçluların en önemli amacı, kişisel bilgilerinizi çalmaya çalışan veya bilgisayarınızı kendi kötü çıkarları için kullanmaya çalışan kötü amaçlı yazılımları indirmenizi sağlamaktır. Bu kötü amaçlı yazılımlar popüler bir oyunun içerisine saklanabileceği gibi, trafik durumunu veya hava durumunu kontrol eden uygulamanın içerisinde de saklı bulunabilmektedir. Dolayısıyla şüpheli gördüğünüz veya güvenmediğiniz sitelere ait uygulamaları indirmemelisiniz.

Güçlü Şifreleri Seçiniz

- Şifreler, tüm internet güvenliği yapısında en büyük zayıf noktalardan biridir. Günümüzde parolalarla ilgili esas problem, insanların siber hırsızların tahmin etmeleri kolay olan şifreler kullanmalarıdır. İnsanlar hatırlanması kolay olan şifreleri seçme eğiliminde olduklarından dolayı şifrelerini basit seçmektedirler. Eğer elektronik aygıtlarınızın ve internet üzerinde bulunan tüm hesaplarınızın güvenliklerini artırmak istiyorsanız siber suçluların tahmin etmesi zor olan güçlü şifreleri seçmeye özen göstermelisiniz. ***Güçlü bir parola belirleyebilmek için, benzersiz kelime grupları oluşturmalı ve en az 15 karakter uzunluğunda, harfleri, sayıları ve özel karakterleri barındıran şifreler kullanmalısınız.***

Virüs Koruma Programınızı Güncel Tutunuz

- İnternet güvenlik yazılımlarınız sizi her tehdide karşı koruyamayacaktır, ancak bu yazılımları güncel tuttuğunuz müddetçe sizi bir çok malware virüslerinden koruyacaklardır. Dolayısıyla, işletim sisteminizin ve kullandığınız başta güvenlik yazılımlarınız olmak üzere tüm uygulamaların güncellemelerini aksatmadan düzenli bir şekilde yapmalısınız.

Alışveriş Yaptığınız Sitelere Dikkat Ediniz

- Çevrim içi bir ürün satın aldığınızda, kredi kartı veya banka hesabı bilgilerinizi kullanmanız gerekmektedir. Dolayısıyla bu bilgileri güvenli, şifreli bağlantılar sağlayan sitelere girmeniz hayati önem taşımaktadır. **Ürün satın almadan önce kart bilgilerinizi gireceğiniz web sitelerinin https: ile başladığından emin olmalısınız. Eğer yalnızca http: ile başlıyorsa o siteden kesinlikle alışveriş yapmamalısınız. Burada sonda bulunan “S” ifadesi secure yani güvenli anlamına gelmektedir.**

İNANMA

İnternette konuştuğun kişiler, kim oldukları hakkında sana yalan söylüyor olabilirler, herkese inanma. İnternette sohbet etmek istiyorsan en iyisi sadece gerçek hayattaki arkadaşların ve ailele sohbet etmektir.

KİŞİSEL BİLGİLERİNİ PAYLAŞMA

İnternette kişisel bilgilerini paylaşırken çok dikkatli ol. Bulduğun yer, telefonun, şifren gibi kişisel bilgilerini asla kimseyle paylaşma ve güvenli kal.

TÜRKÇEYİ DÜZGÜN VE DOĞRU KULLAN

Güzel Türkçemizi koru, düzgün ve doğru kullan. Anlamsız kısaltmalar, yabancı kelimeler, bozuk cümleler kullanma. İnan ki Türkçeyi doğru kullandıkça kendine olan saygın artacak.



DOĞRULA

İnternette edindiğin her bilgi doğru olmayabilir. İnternette yanlış, yanıltıcı ve yönlendirici bilgiler de olduğunu unutma ve bilgiyi farklı web sitelerinden, kitaplardan, kişilerden doğrula.

KABUL ETME

Tanımadığın ve güvenmediğin insanlardan gelen e-posta, mesaj, resim veya dosyaları kabul etme ve açma çünkü virüsler veya hoşuna gitmeyen mesajlar içeriyor olabilir.

AİLENE ANLAT

Eğer internette bir kişi veya bir durum seni rahatsız ediyor veya üzüyorsa ailene anlat. İnternette yaşadığın tüm olumsuzlukları ailene çekinmeden anlatmalısın.

Kaynakça

- www.gim.org.tr
- www.guvenliweb.org.tr
- www.guzelnet.tr
- www.orgm.meb.gov.tr