



Uyanık ol ve siber tuzakları fark et!

Bir web sitesinde,

- **Pop-up** yani aniden açılan küçük pencereler,
 - **Bedava hediyeler** sunan yarışmalar,
 - **Kişisel bilgilerini** isteyen anketler,
 - Bilgisayarına indirdiğinde **zarar verebilecek** programlar,
 - **Satın alabileceğin** bir şeyler varsa,
- Bu sitelere karşı daha uyanık ol!**

E-posta kutusunda,

- **Tanımadığın** kişilerden gelen,
 - **Şifreni** ya da **kimlik bilgilerini** isteyen,
 - İçerisinde bir **bağlantı** (link) ya da **ekinde bir dosya** olan,
 - İçeriğini arkadaşlarına da **göndermeni** isteyen,
 - **Şüpheli** gördüğün e-postalar varsa,
- Bu e-postaları açmadan önce, tekrar düşün.**



Güvenli internet için, Güçlü şifreler oluştur!



Kişisel bilgilerini kullanma.

(Ad-soyad, doğum tarihi, telefon numarası, okul numarası vb.)



En az 8 karakter kullan.



Bazı harfler yerine, sayıları tercih et.

Örneğin: "B yerine 8",
"İ, I, L yerine 1", "S yerine 5",
"O yerine 0", "g yerine 9"



Mutlaka sayı, BÜYÜK-küçük harf ve bir sembol kullan.



Şifrelerini düzenli olarak 6 ayda bir değiştir.



Şifrelerini kimseyle paylaşma.



E-posta hesabından tamamen çıktığından emin ol.

Oturumu kapat



Bir dedektif gibi davran!

Bir web sitesindeki içeriklerin güvenli olup olmadığından emin ol.

İşte sana önemli ipuçları :

Sitenin adresindeki alan uzantısı ile içeriği uyumlu. (org, edu, info vb.)



Ulaşabileceğim iletişim bilgileri var. (Telefon, adres vb.)



Yazılarda dilbilgisi ve yazım hataları yok.



İçeriğin kimin tarafından yazıldığı belirtilmiş.



İçerikler güncel.



Fotoğraflar gerçek.



Site benden kişisel bilgilerimi istemiyor.



Pop-up, anket gibi uygulamalar yok.



