GİZLİ Mİ? GÜVENLİ Mİ?

Bilgisayar ve internet güvenliği için bazı önlemler almamız gerekmekte.

Gerekli şifrelemeler doğru şekilde yapılmalıdır.

Kişisel bilgilerine ulaşılmaması için kişi tarafından belirlenen harf, özel karakter ve sayılardan oluşan parolanın kullanılmasıdır.

Şifrelerinizde kişisel bilgilerinize yer vermeyin.

Örneğin, adınız, doğum tarihiniz veya kimlik numaranız vs. Örneğin ali1999, 32423526655, 1986 ***

- Şifrenizde ardışık sayılar, harfler kullanmayın. Örneğin, 123456, 1234, abcd gibi. ***
- Tahmin edilmesi kolay yan yana bulunan tuşları kullanmayın. Örneğin, qwerty, asdf gibi. ***
- Şifreniz en az 8 basamaklı olsun. ***
- Büyük/küçük harf (A,a…Z,z) ,Rakam (0-9), Noktalama (.,; gibi), Özel karakter (-!+ gibi) içeren şifreler kullanın.

SİBER TUZAKLARI NASIL ANLARIM AFİŞİ

Yukarıdaki tüm bilgileri bilmenize rağmen tamamen güvende sayılmazsınız. Alabileceğimiz birkaç önlem daha var. Bunları aşağıdaki afiş ile kısaca özetledik.

SİBER TUZAKLARI NASIL ANLARIM?

1. İnternette **kimlik bilgilerini** isteyen web sitelerine karşı **dikkatli ol.**
2. **Bedava** hediyelerden, programlardan ve **kazanacağını söyleyen yarışmalardan uzak dur.**
3. Eğlenceli gibi görünen testler, **senin hakkında bilgi toplamak** için hazırlanmış olabilir. **Bir kez daha düşün.**
4. Unutma! Bilinen markalar veya kurumlar e-posta yoluyla senden **parola, kimlik bilgileri gibi kişisel bilgiler istemez.**
5. Açılır pencerelerle **(pop-up)** gelen yarışma ve anketlere **katılma.**
6. **Şüpheli bulduğun e-postaların** içindeki bağlantıya (linke) tıklama ve gönderilen dosyayı **açma.**
7. **Tanımadığın kişilerden** gelen e-postaları açmadan önce, **tekrar düşün.**
8. **İçeriği arkadaşlarına da göndermeni isteyen e-postalar,** seni ve arkadaşlarını riske atabilir. E-postayı sil ve arkadaşlarını **uyar.**
9. **İsteğin dışında** bilgisayar kameranın açılmaması için, kameranı **kontrol et.**
10. Oyun oynamak için, **üye olmanı isteyen siteleri** önce **dikkatlice incele.**