

5.1.7 - GİZLİ ve GÜVENLİ Mİ?

KAZANIMLAR










BT.5.2.3.1. Gizlilik açısından önemli olan bileşenleri belirler.

BT.5.2.3.2. Gizli kalması gereken bilgi ile paylaşılacak bilgiyi ayırt eder.

BT.5.3.3.3. E-posta hesabı oluşturur ve bu hesabını iletişim kurmada kullanır.

Bilgilerimizi korumak için cihazlarımıza şifre koyabiliriz.

Güçlü şifre oluşturma kuralları:

 <p>En az 8 karakter kullanın.</p> <p>*****</p>	 <p>Basit bir kelimenin içerisindeki harf ve rakamları değiştirebilirsiniz.</p> <p>Örneğin: B yerine 8, İ, I, L yerine 1, S yerine 5, O yerine 0, g yerine 9</p>
 <p>Şifrenize mutlaka sayı, BÜYÜK-küçük harf ve bir sembol ekleyin.</p> <p>Örneğin, Bilgisayar yerine 81LG1S@y@</p>	 <p>Şifre belirlerken önce, unutmayacağınız bir cümle oluşturun.</p> <p>Örneğin, sevdiğiniz bir şarkıda geçen ya da bulduğunuz yeni bir cümleyi şu şekilde kullanabilirsiniz. 'Bugün bayram, erken kalkın çocuklar' 8uGün.8@yr@m!</p>
 <p>Belirli bir güvenli parola bulun. Farklı siteler ya da e-posta adresleriniz için, kullandığınız siteye özel olarak ek sembol, harf ya da sayı ekleyin.</p>	 <p>Örneğin, şifreniz: parola1 e-posta şifreniz: parola1mail@ sosyal medyada kullanacağınız şifreniz: parola1twtr olabilir.</p>
 <p>Sözlükten alınan bir sözcük kullanmayın!</p> <p></p>	 <p>Hiçbir özel kimlik bilgisi kullanmayın!</p> <p>(Ad-soyad, e-posta, telefon, kimlik numarası, doğum tarihi, okul numarası vb.)</p>

5.1.7 - GİZLİ ve GÜVENLİ Mİ?



Kolayca tahmin edilebilecek bir parola kullanmayın!

(Örneğin, okulun adı, tuttuğun takımın adı, evcil hayvanın adı vb.)



GÜVENLİKLE İLGİLİ ÖNEMLİ KURALLAR



Parolanızı düzenli olarak, en az 6 ayda bir değiştirin.



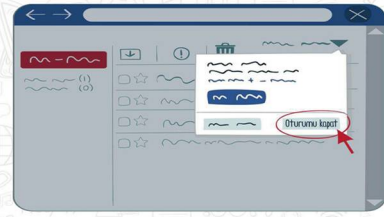
Arkadaş listenizi ve bilgisayarınızı koruyun.



Başkasının bilgisayarında, okulda veya internet kafede kullandığınız bilgisayarlarda 'Beni hatırla' seçeneğini kullanmayın.



Oturumunuzu kapatmayı unutmayın.



Şifrenizin başkası tarafından kullanıldığını düşünüyorsanız, güvenli doğrulama yolları ile şifrenizi sıfırlayın.



İşte benim güvenli şifrem: (zor şifre oluştururken hatırlamayacağım bir şifre seçmiyorum!!)

5.1.7 - GİZLİ ve GÜVENLİ Mİ?

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 **istememez.**
- 5 Açılır pencerelerle (**pop-up**) gelen **yanışma** 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.**

POP-UP
KATILI
HEDİYELER
KAZAN
KİMLİK BİLGİLERİ
SİRELER