



Parola Güvenliği

Kurumsal e-posta hesapları ve birimler tarafından sunulan servislere (kullanıcı bilgisayarlarının işletim sistemi erişimleri, web servisi erişimleri vb.) kullanıcı hesabı ve parola ile yapılan kimlik doğrulamalarında dikkat edilmesi gereken hususlar aşağıda belirtilmiştir:

1. Parolaların Güçlü Yapıda Oluşturulması:

Parola tanımlama ya da parola değişikliği işlemlerinde güçlü parolalar oluşturulmalıdır. Bu amaçla güçlü parola yapısına uygun seçimler yapılması için gerekli talimatlar aşağıda belirtilmiştir:

- Parola, en az 8 (sekiz) karakterli olmalıdır.
- İçerisinde en az 1 (bir) tane büyük ve en az 1 (bir) tane küçük harf bulunmalıdır.
- İçerisinde en az 1 (bir) tane rakam bulunmalıdır.
- İçerisinde en az 1 (bir) tane özel karakter bulunmalıdır (@, !, ?, +, \$, #, &, /, {, *, vb.).
- Aynı karakterler peş peşe kullanılmamalıdır (aaa, 111, XXX vb.) ve ardışık tekrarlardan kaçınılmalıdır (ababab vb.).
- Kelime veya rakam olarak sıralı (ardışık) karakterler kullanılmamalıdır (abcd, asdf, aaabbb, qwerty, zxcvb, 12345678, 123321 vb.).
- Kişisel bilgiler gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır (Örneğin; ad, soyad, doğum tarihi, aile bireylerinin isimleri, çocuk adı, çocuk doğum tarihi, telefon numarası veya adres bilgileri vb.).
- Çoğu kişinin kullanabildiği, aynı veya çok benzer yöntemlerle geliştirilmiş tahmin edilebilir kombinasyonlar kullanılmamalıdır.

- Birden çok bilgisayarda veya uygulamada aynı kullanıcı adı ve parola kombinasyonu tercih edilmemelidir.
- Kurum içi ve kurum dışı hesaplar için kullanılan parolalar aynı olmamalıdır.

2. Parolaların Belirli Sürelerde Değiştirilmesi:

- Parola yenileme süresi 90 günü geçmemelidir.
- Herhangi bir tehdit veya ihlal şüphesi algılanması durumunda parolalar derhal değiştirilmelidir.

3. Parolaların Gizliliği ve Korunması:

- Hesap bilgileri ve parolalar hiçbir şekilde başkaları ile paylaşılmamalı, başkaları tarafından ele geçirilmemesi için güvenli şekilde korunmalıdır.
- Parolalar; başkalarının görebileceği şekilde kâğıtlara yazılmamalı, fiziki alanlarda bırakılmamalı ve şifresiz/güvensiz dijital ortamlarda saklanmamalıdır.
- Kurumsal e-posta ve kullanıcı hesaplarının korunması ile güvenli bir şekilde saklanması, tamamen kullanıcının sorumluluğundadır.