

Şifre Seçiminde Dikkat Edilmesi Gereken Hususlar

İyi Bir Şifre Nasıl Seçilir

Çoğu zaman iyi bir şifre seçmek kullanıcılara zor gelebilir. Bunun için aşağıda bazı ipuçları verilmiştir.

- Şifreniz en az 6 karakter uzunluğunda olmalıdır. Bu brute-force olarak adlandırılan kombinasyon deneme tipi saldırılarda, saldırganları yıldırmak için yeterli bir uzunluktur. Şu an, bir çok Unix/Linux sisteminde maksimum şifre uzunluğu sekiz karakterdir. Daha fazla karakter girmek istediğinizde, sekizinci karakterden sonra girilen karakterler yoksayılır. (Örneğin; “abN0rmaLbrAin” şifresinin sekizinci karakterinden sonra girilen karakterler yoksayılarak “abN0rmaL” şeklinde kabul edilir.)
- İyi bir şifre genellikle; karışık biçimde sıralanmış büyük-küçük harfler, numaralar, noktalama işaretleri ve en az 6 karakterden oluşmalıdır. Maalesef, bazı kullanıcılar hatırlanması zor şifreleri bir yerlere yazar. Bunun sonucunda başka kişiler tarafından şifreniz kolayca öğrenilir. Böyle bir durumla karşılaşmamak için şifrenizi herhangi bir yere yazmayınız.
- “*License plate*” kuralı: Plaka numarası veya herhangi bir cümleyi şifre yapmak istediğinizde onu sekiz karakter olacak şekilde sınırlayın. Örneğin: “Artık kısa cümleler kuruyorum” şeklindeki cümleyi “aKısa2CK” şeklinde bir şifreye dönüştürebiliriz.
- Bir kelimeyi noktalama işaretleri ile ayırarak (Örneğin: “vega%tarian”)
- Herhangi bir cümlenin birinci-ikinci veya son karakterini alıp, yeni bir kelime oluşturup bunu şifre olarak kullanabilirsiniz. Örnek: “*You can't always get what you want*” cümlesinde bulunan kelimelerin ilk harflerini alarak “ycagwyw” kelimesini oluşturabilirsiniz. Büyük harf ve bir veya iki numara ilave edip “yCag5wyw” şeklinde kırılması oldukça zor bir şifre oluşturabilirsiniz.
- Bilerek bir kaç yazım hatası yaparak şifrenizin kırılmasını zorlaştırabilirsiniz (Örneğin; “Protect” --> “Port7cet”).

Üstteki tekniklerden en az bir kaçını kullanarak iyi bir şifre elde edebilirsiniz. En iyi şifrelerden biriside sizden başka kimsenin anlayamayacağı, başkalarına tamamen karışık gelen şekilde seçilmiş olandır.

Olmaması Gereken Şifreler

Şifre kırıcıların kolayca ele geçirebileceği şifre türleri;

- Sözlükte bulunan kelimeler.
- Herhangi bir sözlükte (Yabancı dil, Tıbbi terimler, vs..) bulunan kelimeler
- Kullanıcı adınız. (User name)
- İsminiz, soyisminiz
- Eşinizin ismi
- Herhangi birisinin ismi, soyismi (Şifre kırıcıları annenizin kızlık soyismini, yada herhangi bir akrabanızın ismini bilmeyebilir. Fakat içinde 100,000 isim bulunan bir listeden, bunların herbirini denemesi yeterlidir.)
- Şifre kırıcıların, şifreleri kırmakta kullandıkları *wordlist*'leri (kelime listeleri) vardır. Bu listelerde bir çok insanın kullandığı şifreler mevcuttur. Bunlardan bazıları;

Kısaltmalar, gezegen isimleri, terimler, çizgi film karakterleri, karakter modelleri, makine isimleri, ünlü isimleri, kız-erkek isimleri, film adları, sayılar, kısa cümleler, yer isimleri, bilim-kurgu, şarkılar, sporlar, soyisimler...

- Üstte bulunan kelime grubunda bulunan herhangi bir kelimenin önüne/sonuna tek karakter getirilmesi ile oluşturulan şifreler. (“8dinner”, “happy1”, 2unlimited1”)
- Üstte bulunan kelime grubunda bulunan herhangi bir kelimenin büyük harfle yazılması ile oluşturulan şifreler. (“cat” --> “Cat”).
- Eskiden iyi bir şifre yaratma tekniği olarak, bazı karakterleri benzer rakamlarla değiştirilmesi (örneğin o harfi yerine 0 rakamı) önerilirdi, ancak günümüzde şifre kırıcıların yeteneklerinin gelişmesiyle bu iyi bir korunma yöntemi olmaktan çıkmıştır.
- “foobar”, “xyzyzy” ve “qwerty” gibi popüler şifrelerde normal kelime gibi *wordlist*'lerde bulunabilir. Şifre kırıcılar bu kelimeleri de aramaktadır.