

Parolalarınız nasıl çalınır ve sistem güvenliğinizi nasıl sağlarsınız.

Yakalama

Parolalar ağız üzerinden
iletilirken ele geçirilebilir.



Kaba-Kuvvet Tekniği

Otomatik parola tahmin etme ile
parolanız elde edilebilir.



Araştırma

Elektronik ortamda
depolanan parolaları bulmak
için BT altyapısı taranabilir.



Parola Çalma

Bilgisayarınıza yakın bir yere
yazdığınız el yazması parolalarınız
çalınabilir.

Tahmin

İsim, doğum tarihi, kimlik
gibi bilgiler parola
tahminlerinde kullanılabilir.



Omuz Sörfü

Parolalarınızı yazarken
birisi gizlice izleyebilir.



Sosyal Mühendislik

Saldırganlar parolaları elde
etmek için sosyal mühendislik
tekniklerini kullanabilir.



Klavye Dinleme

Bilgisayarınıza yüklenmiş
keylogger basılan klavye
tuşlarını kaydeder.



Kullanıcıların parolaları ile başa çıkmalarına yardımcı olun

- Sadece ihtiyaç duyulan parolaları kullanın.
- Kullanıcılar üzerindeki yükü azaltmak için teknik çözümler kullanın.
- Kullanıcıların güvenli bir şekilde parolalarını kaydetmelerini ve saklamalarını sağlayın.
- Kullanıcılardan yalnızca, benzeme şüphesi bulunduğunda parolalarını değiştirmelerini isteyin.
- Kullanıcıların kolay ve hızlı bir şekilde parolayı sıfırlamasına izin verin.

Güçlü parola nasıl üretilir?

- Mümkün olduğunca en az 10 karakter kullanın.
- Parolalar kesinlikle klavye tuş sırasını takip eden (ardışık) karakterlerden oluşmamalıdır.
- Harflerin yanı sıra, rakam ve "? , @ , ! , # , % , + , - , * , %" gibi özel karakterlerde kullanın.
- Bilinen kısaltmaları ve kelimelerin tersten yazılmış hallerini kullanmaktan kaçının.
- Her şey için aynı parolayı kullanmayın.



Sık kullanılan parolaları
kara listeye alın.



Başarısız giriş denemelerini
izleyin.



Yönetici ve uzak kullanıcı
hesabı parolalarınıza dikkat
ediniz.



Parolalarınızı açık şekilde
saklaMAyınız.

**** Güncelle

Aygıtlar veya yazılımların
üreticileri tarafından atanan
parolarlarını değiştirin.

Kaba kuvvet saldırılarının
önlenmesi için kısıtlama,
denetleme ve kilitleme
uygulayın.

