

GÜVENLİ İNTERNET EMET İÇİM:



Basit parolalar kullanmayın!

İnternet dünyasında yapılan en önemli hata basit parolalar kullanmak veya bir parolayı birkaç platformda aynı şekilde kullanmaktır. Bu durum siber saldırganlar için bulunmaz bir fırsat sağlar. Seniseviyorum, 123456, sevgilim, password1 gibi basit parolaların çok çabuk bir şekilde kırılabileceğini düşünmemiz gerekiyor. Bu tarz basit parolalar birkaç saniye içerisinde kırılarak sistemlere veya hesaplarınıza yetkisiz erişim elde edilmesine sebep olacaktır.

"Basit parolalar şifre kırıcı uygulamalar sayesinde birkaç saniye içerisinde kırılabilir!"

Aynı zamanda internette birçok yere üye olduğumuzu ve bu platformların da hacklenebildiğini unutmayın. Birçok kullanıcının yaptığı en önemli hata aynı şifreyi her yerde kullanmaktır. Parolanız ne kadar gelişmiş ve karmaşık olursa olsun, eğer bir parolayı birçok platformda kullanıyorsanız bu platformlardan biri hacklendiğinde parolanızın da elde edilebileceğini hatta birçok web sitesinin parolaları açık text olarak tutulduğunu yaşanan hack vakalarında görmekteyiz. Bu noktada basit parolalar yerine güçlü parolalar kullanmanızı ve parolaların tek kullanımlık olması gerektiğinin altını çizmek istiyoruz.

İşletim Sistemlerinizi güncel tutun

İşletim sistemleri kullanmış olduğunuz cihazların yönetimini ve işlerliğini sağlamaktadır. İşletim sistemlerinin (Windows, Linux, MacOS) güncellemeleri ise, tespit edilen hatalar ya da ortaya çıkabilecek güvenlik zafiyetlerine karşı sisteminizi güvenli ve stabil durumda tutmak için yayınlanır.

Mobil, dizüstü veya masaüstü bilgisayarlarınızda bu güncellemeleri yapmalı ve güvenliğiniz için sistemlerinizi güncel tutmak zorundasınız. Aksi takdirde işletim sistemlerinde tespit edilen zafiyetler sebebi ile saldırganlara bir arka kapı açılabilir ve güncelleme yapmadığınız için her an bir siber saldırıya maruz kalabileceğinizi unutmayın.

E- postalara dikkat edin!

E-postalar günümüz internet dünyasının en önemli iletişim araçlarından biri haline gelmiştir. Hem kurum tarafında hem de kişisel kullanımda e-postalar siber saldırganların sisteme erişmelerinde önemli rol oynamaktadır.

Sahte e-postalar veya sahte bağlantıların açılması kurbanların birkaç saniye içerisinde siber saldırıya maruz kalmalarına neden olabilir. Bu noktada tanımadığınız kişilerden gelen e-postaları açarken dikkatli olmanızı, kısaltılmış URL olarak gönderilen bağlantılara tıklamamanızı ve kimliği belirsiz kişilerden gelen e-postalardaki tehdit, heyecan veyahut şantaj içeren metinlere dikkat etmeniz gerekiyor. Siber saldırganlar sistemlere erişmek için sahte e-postalar içerisinde zararlı bağlantılar gönderebildiği gibi virüslü dosyalar veya makro içeren zararlı dokümanlar da iletebilir.

Gelen e-postalarda zararlı yazımların kurulmasına imkan tanıyan .EXE, .Jar veya benzeri çalıştırılabilir biçimdeki dosya uzantılı eklerini açmamanız, sahte bağlantılara tıklamamanız internet güvenliğindeki en önemli güvenlik önlemlerinden biridir.



