KeePass Nedir?

- KeePass Nedir?
- Neden Kullanılır?
- Çalışma Mantığı
- KeePass Şifreleri Nerede Saklar?

KeePass Nedir?

KeePass, temel anlamda bir şifre saklama programıdır. Detaylarına bakacak olursak; kullanıcıların, tüm şifrelerini oluşturulan veri tabanında tutup tek bir platform üzerinden erişim sağlayarak kolaylık ve güvenilirlik açısından kullanıcıları memnun etmeyi hedefleyen açık kaynak kodlu bir programdır.

Neden Kullanılır?

Teknolojinin gelişmesiyle birlikte artık her işimizi internet üzerinden yapmaktayız. Öyle ki bankacılıkişlemlerinden fatura ödeme işlemlerine, çevrimiçi alışverişten internet üzerinden çalışıp gelir elde etmeye kadar her işimizi internet üzerinden gerçekleştiriyoruz. Her işimizi internet aracılığıyla yapınca haliyle tüm bilgilerimizde internet ortamına taşınmış oluyor.

Her mecranın kötü niyetli insanları olduğu gibi internet ortamının da kötü niyetli insanları var tabiki. Bu insanlara ‘siyah şapkalı hacker’ diyoruz. Bu kişiler internet üzerindeki bilgilerinize ulaşmak için çeşitli yollar denerler. Bunlardan biri keylogger olarak tanımladığımız zararlı bir yazılımdır.

Bu yazılım sisteminize bulaştığı zaman ister fiziki klavye olsun ister sanal klavye olsun bastığınız her tuşu izler ve kaydeder. Böylelikle kötü niyetli hacker girdiğiniz bilgileri öğrenip verilerinize kolaylıkla erişebilir.

İşte KeePass tam olarak bu noktada devreye giriyor. Hesap bilgilerinizi girerken kopyala yapıştır mantığı ile çalıştığı için sisteminize sızmış bir hacker olsa bilse giriş bilgilerinizi göremez ve bilgileriniz bu anlamda güvende olur.

İnternet ortamında kullandığımız şifreleri yönetebilmek için KeePass oldukça güzel bir alternatif. Hem güçlü şifre üretmekte hem de onları saklamakta oldukça kolaylık sağlıyor. Her hesap içinfarklı ve güçlü şifreler oluşturarak hesaplarınızın güvenilirliğini artırmaya da olanak tanıyor.

Açık kaynak kodlu olması, uçtan uca şifreleme, çapraz platform ve senkronizasyon, 2 faktörlü doğrulama, eklenti aracılığıyla tarayıcı entegrasyonu ve çoklu şifreleme seçenekleri özellikleri ile Keepass kullanıcılara teknolojiyi güvenle kullanmanın keyfini veriyor.

Çalışma Mantığı

Çalışma mantığını adım adım inceleyelim.

Birinci adım olarak; Kullanıcı "veri tabanı" oluşturur. Bu veri tabanı, tüm şifreleri ve diğer hassas bilgileri içerir.Veri tabanı oluşturulurken kullanıcıdan bir "ana parola" veya "anahtar kurtarma dosyası" gibi bir ana erişim yöntemi belirlemesi istenir.

Daha sonrasında ise kullanıcı, çeşitli kayıtları (örneğin, web siteleri, uygulamalar, hesaplar) ve bu kayıtlara ait kullanıcı adları ve şifreleri veri tabanına ekler. Eklenen bilgiler, veri tabanında "giriş" olarak kaydedilir.

KeePass, eklenen bilgileri güvence altına almak için AES (Advanced Encryption Standard) gibi güçlü şifreleme algoritmalarını kullanır. Ana parola veya anahtar kurtarma dosyası, bu şifreleme işleminde kullanılır. Veri tabanı içeriği, şifrelenmiş bir biçimde diskte saklanır. Bu sayede verilerin güvenliği sağlanmış olur.

Ana parola veya anahtar kurtarma dosyası, gerçek şifreleme anahtarı olarak kullanılmadan önce güvenli bir biçimde saklanır. Anahtar türetme işlemi, kullanıcının girdiği ana parolayı veya anahtar kurtarma dosyasını temel alarak gerçek şifreleme anahtarını türetir. Bu, veri tabanının şifresini çözmek için gereklidir.

Kullanıcı, KeePass uygulamasını başlattığında veri tabanına erişmek için ana parolasını girmesi veya anahtar kurtarma dosyasını sağlaması istenir. Girilen ana parola veya kullanılan anahtar kurtarma dosyası, gerçek şifreleme anahtarının türetilmesi için kullanılır. Doğru ana parolası veya anahtar kurtarma dosyası sağlandığında, veri tabanı açılır ve içeriği kullanıcıya görüntülenir.

Kullanıcı, veri tabanı içinde saklanan kayıtlardan birini seçerek ilgili kullanıcı adı ve şifreyi elde eder. Bu bilgileri kopyalayarak veya otomatik olarak ilgili hesaba giriş yapabilir.

KeePass Şifreleri Nerede Saklar?

KeePass, kullanıcıların şifrelerini ve diğer hassas bilgileri güvenli bir şekilde saklamak için bir veri tabanı kullanır. Bu veri tabanı, kullanıcının belirlediği bir ana parola veya anahtar ile korunur. Veri tabanı, kullanıcının bilgisayarında veya bulutta saklanabilir. Bazı kullanıcılar, USB sürücüler veya harici depolama aygıtları gibi taşınabilir ortamlarda KeePass veri tabanını taşıyabilirler. Bu seçenek, farklı cihazlar arasında veri tabanını taşımak veya yedeklemek için kullanılabilir. KeePass'ın bazı sürümleri, veri tabanını özel bir sunucuda saklama ve uzaktan erişim sağlama yeteneği sunabilir. Bu, birden çok cihaz arasında senkronizasyon yapmayı kolaylaştırabilir. Bu yöntemde de güvenlik dikkat edilmesi gereken bir faktördür.