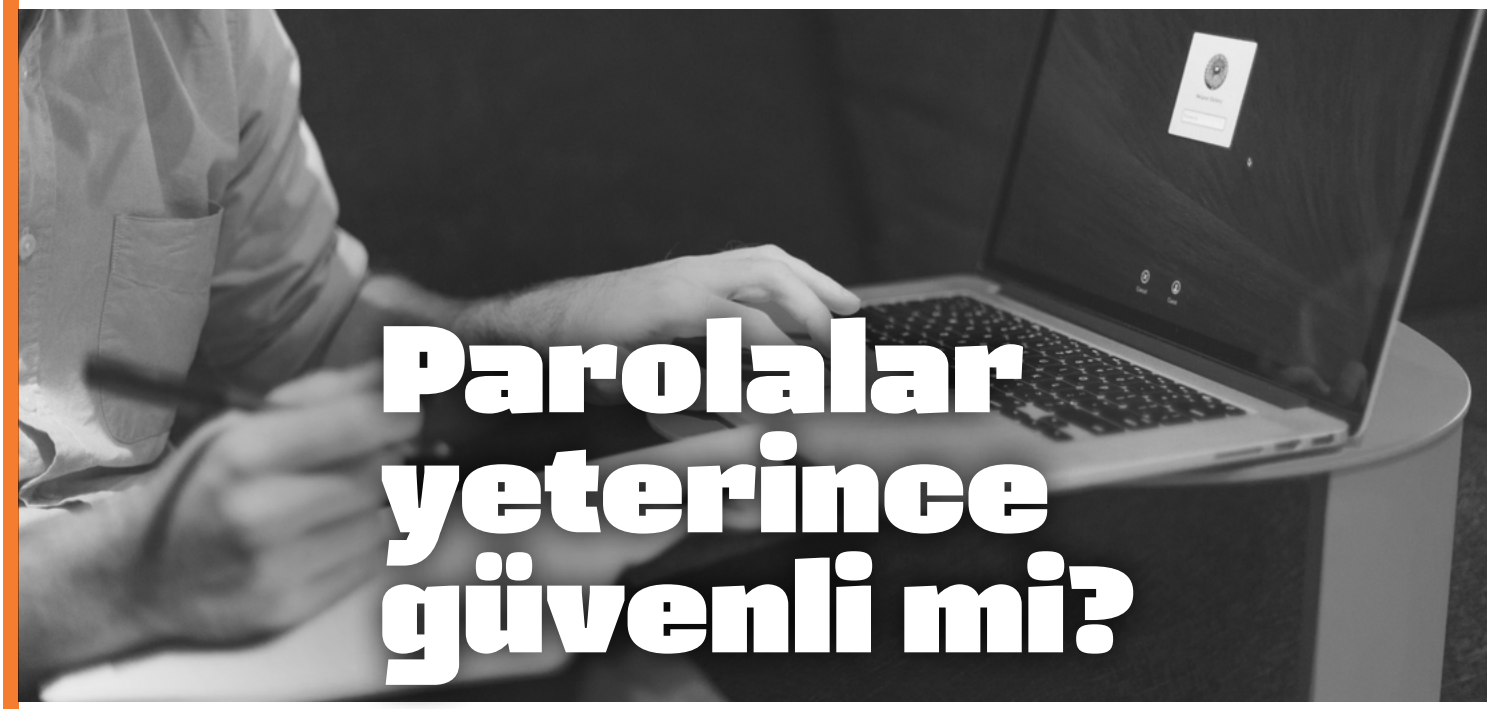
GÜVENLİ GÜNLER BÜLTENİ

Bilgisayar kullanıcılarına yönelik hazırlanır. Her ayın 15'i çıkar. Bültenlerin her ay size ulaşması için üye olunuz: http://eepurl.com/bP-tWn

AĞUSTOS 2016



Parolalar yeterince güvenli mi?

PAROLALAR UZUN YILLARDIR ELEKTRONİK ORTAMLARDA KİMLİK DOĞRULAMAK İÇİN KULLANILMAKTADIR. *Bu görevlerini uzun süredir genel olarak başarıyla sürdürmüşlerdir ama artık tek başlarına kullanıldıklarında güvenliği sağlamakta yetersiz kalmaktadırlar.* Wired *dergisi editörü Mat Honan'ın tüm sosyal medya hesapları ele geçirildikten sonra söylediği gibi,*

"Ne kadar uzun olursa olsun, ne kadar karmaşık olursa olsun, parolalar tek başına sizi koruyamaz."

Parolaların bazı zayıf yanları vardır. Örneğin tahmin edilebilirler, bilgisayarlarımıza ya da mobil cihazlarımıza yüklenen klavye dinleme sistemi (keylogger) gibi zararlı yazılımlar ile çalınabilirler ya da güvenli olmayan ağlar üzerinden ele geçirilebilirler. Hatta uygulamaların parola veritabanlarına sızılıp, milyonlarca kişinin parolası bir anda ele geçirilebilir. Bu zayıflıklar nedeniyle artık birçok uygulamada sadece parola ile yetinilmemekte, parolanın yanında ikinci bir farklı bileşenin daha bulunması kimlik doğrulama için zorunlu tutulmaya başlanmıştır. Bu uygulamalara "iki faktörlü kimlik doğrulama" adı verilmektedir.

PEKİ, İKİ FAKTÖRLÜ KİMLİK DOĞRULAMA NEDİR VE BİZE NE YARAR SAĞLAR?

İki faktörlü kimlik doğrulama, birbirinden bağımsız iki faktörün art arda kullanılması ile kimlik doğrulama yapmak demektir. Birbirinden bağımsız bu faktörler aşağıda belirtilen 3 gruba ayrılırlar:

- Bildiğimiz bir şey: Örneğin Parola.
- Sahip olduğumuz bir şey: Örneğin Kredi Kartı, Cep Telefonu, Tek Kullanımlık şifre cihazı vb.
- Biyometrik bilgilerimiz: Örneğin sesimiz, göz retinamız, parmak izimiz ya da el damar haritamız.

Bir örnek olarak ülkemizdeki internet bankacılığı verilebilir. İnternet bankacılığında iki faktörlü kimlik doğrulama yapmak mevzuat gereği zorunludur. Dolayısıyla, internet bankacılığı parolasına ek olarak SMS ile gönderilen tek kullanımlık şifre kullanımı veya bankaların sunduğu tek kullanımlık şifre üreten uygulama kullanımı, iki faktörlü kimlik doğrulamaya güzel bir örnektir.

Bir diğer örnek de Google'ın sunduğu iki adımlı kimlik doğrulamadır. Hesabınız için bu özellik etkinleştirildiğinde, kimliğinizi doğrulamak için parolanıza ek olarak kayıtlı cep telefonunuza gönderilen tek kullanımlık şifreyi de doğru girmeniz gerekmektedir. Parolaların zayıf yönleri göz önüne alındığında, parolanın başkalarınca ele geçirilmiş olması durumunda bile ikinci faktörün sorulmasının hesapların güvenliğini oldukça artırdığı açıktır.

Uygulamalar destekledikçe iki faktörlü kimlik doğrulamayı etkin hale getirmek yararlıdır. Bazı uygulamalar ise ne yazık ki sadece parola kullanımını desteklemektedir ve bu uygulamalarda yukarıda sözü edilen riskler geçerliliğini korumaktadır. Ancak ister kimlik doğrulama için tek başına kullanılıyor olsun, isterse iki faktörlü kimlik doğrulama unsurlarından birisi olsun, kendimizi daha iyi koruyabilmek için parolalarımızı aşağıdaki güvenlik tavsiyelerine uygun şekilde oluşturmakta ve saklamakta yarar vardır.

Parolalar için Güvenlik Tavsiyeleri

- Parolanız sizin hatırlayabileceğiniz ama başkasının tahmin edemeyeceği şekilde olmalıdır.
- Parolanız mümkün olduğunca uzun olmalıdır, 8 karakterden kısa parolalar daha kolay ele geçirilir.
- Parolalar karmaşık olmalıdır, içinde büyük harf, küçük harf, rakam ve mümkünse özel karakter bulunmalıdır.
- Parolalar sözlüklerde yer alan kelimelerden oluşmamalıdır.
- Parolalar diş fırçasına benzetilebilir, hiç kimseyle paylaşılmamalıdır ve periyodik olarak değiştirilmelidir.
- Parolalar hiçbir yere yazılmamalıdır.
- Her sistemde veya uygulamada farklı parola tercih edilmelidir. Sosyal medya uygulamalarında buna çok dikkat edilmelidir.
- Tarayıcıların "Parola Hatırla" özelliklerinin yeterince güvenli olmadığı bilinmelidir.
- Parola sıfırlamak için kullanılan güvenlik sorularının yanıtlarında da benzer şekilde dikkatli davranılmalıdır.

↓

» Parolaların ele geçirilmesini zorlaştırmak için bilgisayar ve mobil cihaz güvenliğine dikkat edilmelidir.
  - Bilgisayarlar ve mobil cihazlar sürekli güncel sürümde kullanılmalıdır ve üreticilerin yayınladığı güvenlik yamaları yüklenmelidir.
  - Üzerlerinde uç nokta güvenliği yazılımları kullanılmalıdır ve bu yazılımlar da sürekli güncel tutulmalıdır.
  - Lisansı kırılmış yazılımlar bilgisayarlarımıza zarar verebileceği için kullanılmamalıdır.
  - Mobil cihazlara sadece resmi uygulama marketleri üzerinden uygulama yüklenmelidir.
  - Mobil cihazlar yazılımları kırılarak (Jailbreak ya da rooted) kullanılmamalıdır.
  - Ekran koruyucu politikası uygulanmalıdır ve ekran koruyucu devreye girdiğinde parola ile korunmalıdır.
  - Güvenli olmayan ağlar kullanılmamalıdır. Örneğin herkesin kullanımına açık kablosuz ağlarda bilgilerinizin güvenliğini sağlayamayabilirsiniz.
  - Ömrünü doldurmuş cihazlar, içindeki bilgiler geri döndürülemeyecek şekilde imha edilmeden başkasına verilmemelidir ya da çöpe atılmamalıdır. Buna dikkat edilmediğinde bilgiler kolaylıkla başkaları tarafından ele geçirilebilir.

» Son olarak da, güvenlik farkındalığınızı sürekli yüksek tutmanız yararlı olacaktır. E-posta ve sosyal medya uygulamaları ya da telefon ile yapılan sosyal mühendislik saldırılarına karşı dikkatli olunmalıdır.

YAZAR HAKKINDA

Aydın Küçükkarakaş, bilgisayar mühendisliği mezunu olup son 10 yıldır bilgi güvenliği üzerine çalışmaktadır.