İki adımlı doğrulama nasıl çalışır?



www.yzokul.com.tr

İki adımlı doğrulama nasıl çalışır?



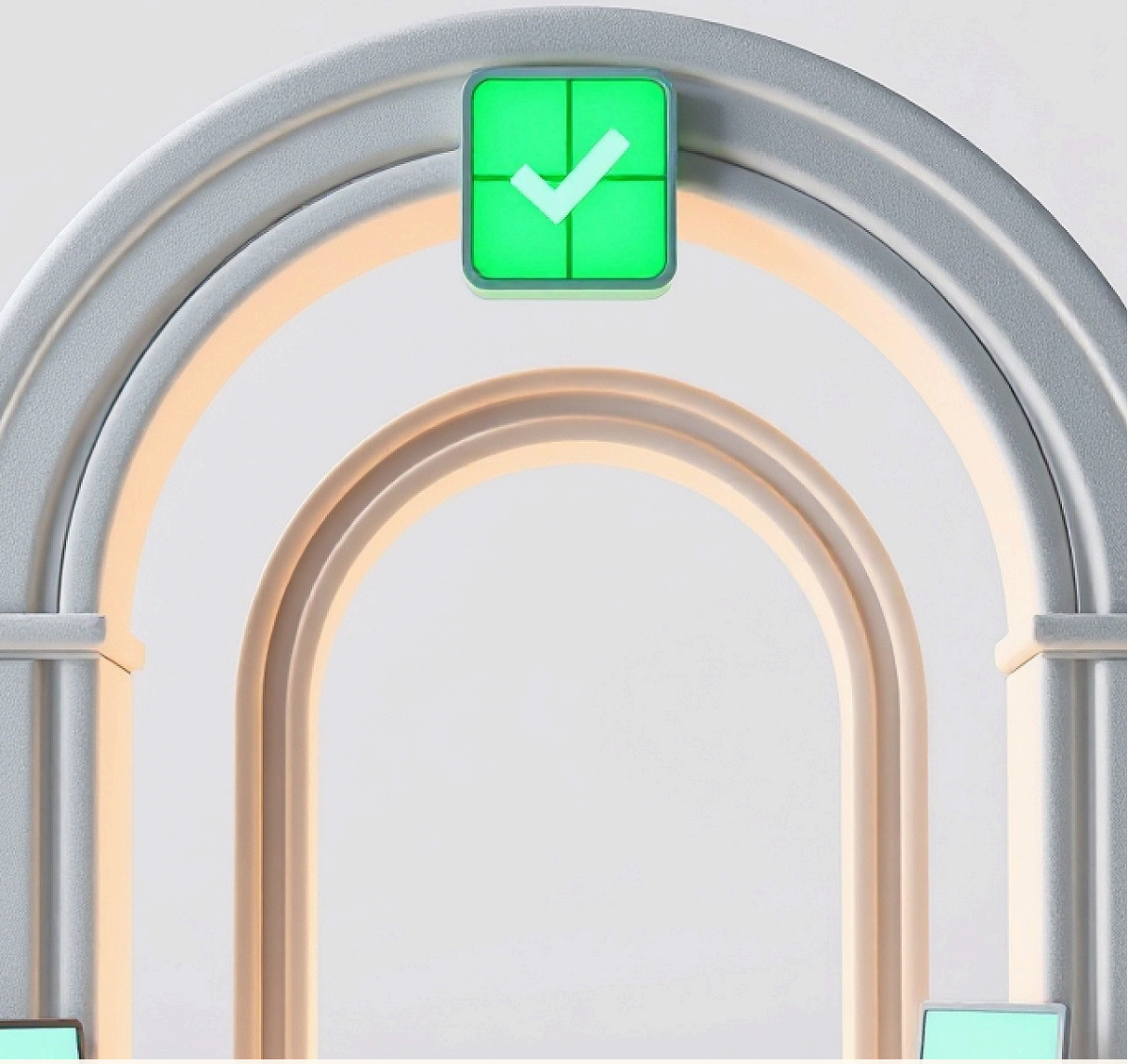
Bir hesaba giriş yaptığında genellikle bir parola yazarsın. İki adımlı doğrulama, girişin parolanın yanı sıra ikinci bir kontrol gerektirebileceği anlamına gelir. İçeri girmek için yalnızca parolayı bilmek her zaman yeterli değildir. İkinci kontrol, telefonuna gönderilen bir kod gibi ekstra bir şeydir. İçeri girmene izin verilmeden önce her iki kontrolün de geçmesi gerekir.



Parola, kim olduğunu kanıtlamak için yazdığın gizli bir sözcük veya ifadedir. Girişteki ilk kontroldür. Hesabını oluştururken belirlersin ve gizli tutarsın. Sistem, yazdığın şeyi sakladığı şeyle karşılaştırır. Eşleşirlerse ilk kontrol geçer. Parola, bildiğin bir şeye dayanan bir kanıt türüdür.



Başka biri parolanı öğrenebilir veya tahmin edebilir. Seni kandırarak açıklamana yol açabilir ya da bir veri ihlalinde bulabilir. Parola tek kontrolse, onu bilen herkes senin yerine giriş yapabilir. Bu yüzden tek başına bir kontrol başarısız olabilir. Sızmış bir parola hesabını açmak için yeterli olmamalıdır.



Bir giriş, parolanı ve ardından bir kontrol daha isteyebilir. Girişe izin verilmeden önce her ikisi de geçmelidir. Önce parolanı yazarsın ve sistem onu kontrol eder. Sonra ikinci kanıtı, örneğin bir kodu veya bir onayı ister. Giriş ancak her ikisi de doğru olduğunda tamamlanır. İki adımlı doğrulamanın özü budur.



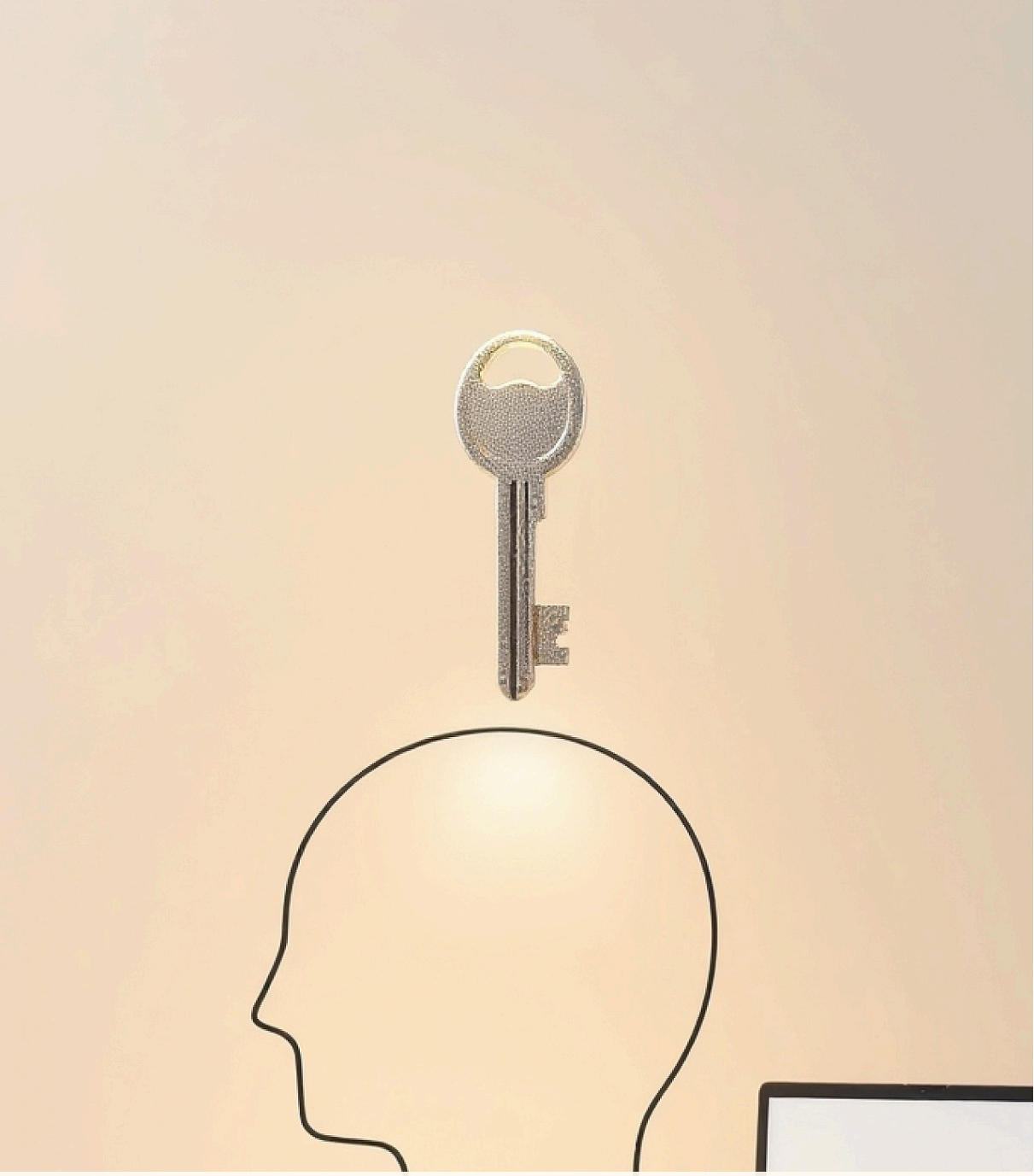
Parolanı girdikten sonra telefonun gibi ayrı bir cihazda bir doğrulama isteği görünebilir. Girişi tamamlamak için orada onaylarsın. İstek, onaylamak için basit bir dokunuş veya yazdığın bir kod olabilir. Ayrı cihaz, yalnızca parolanın sağlamadığı bir şeye sahip olduğunu kanıtlar. O cihazda onaylamak ikinci kontroldür.



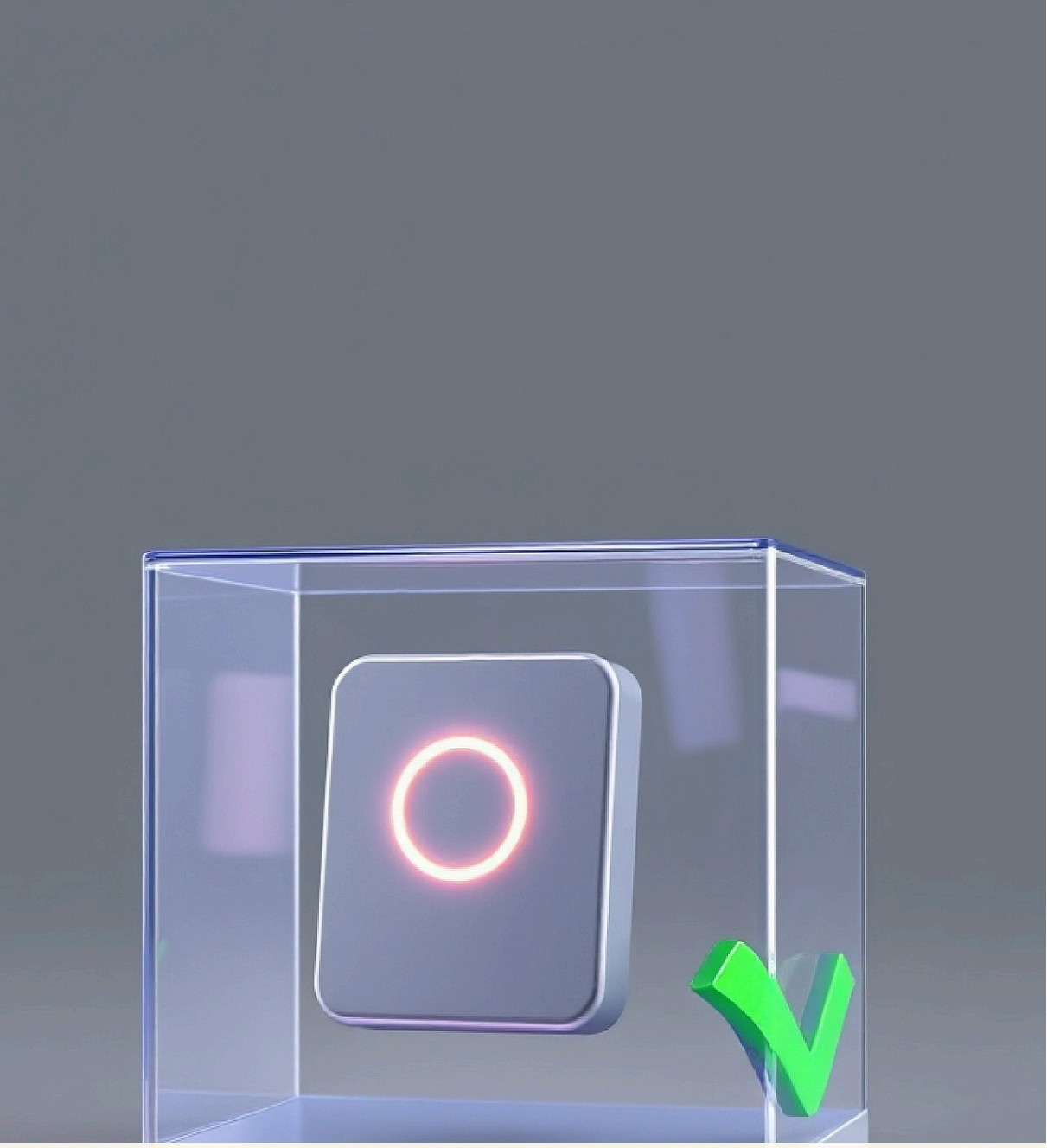
İki kontrol farklı kanıt türleri olmalıdır. Yaygın bir eşleşme, bildiğin bir şey artı sahip olduğun bir şeydir. Bildiğin bir şey parola veya PIN'dir. Sahip olduğun bir şey telefonun veya bir güvenlik anahtarıdır. İki farklı tür kullanmak girişi güçlendirir. Her iki kontrol de aynı türdense fayda daha küçüktür.



İki farklı parola istemek hâlâ yalnızca tek bir kanıt türüdür. İkisi de bildiğin bir şeydir. Bir parola sızarsa diğeri de sızabilir veya tahmin edilebilir. İki parola illa iki farklı doğrulama faktörü değildir. İki faktör elde etmek için ikinci kontrol, sahip olduğun bir şey gibi farklı bir tür olmalıdır.



Bildiğin bir şey, zihnindeki bilgiye dayanan kanıttır. Örnekler arasında bir parola, bir PIN veya güvenlik sorularının yanıtları yer alır. Bu, yaygın iki adımlı kurulumdaki ilk faktördür. Kendini kanıtlamak için onu yazarsın veya söylersin. Bilgiye dayalı kanıtın kullanımı kolaydır, ancak unutulabilir veya biri öğrenirse çalınabilir.



Sahip olduğun bir şey, elinde bulundurduğun bir nesneye dayanan kanıttır. Örnekler arasında telefonun, bir güvenlik anahtarı veya akıllı kart yer alır. Bu, genellikle ikinci faktördür. Girişi onaylamak için nesneyi kullanırsın, örneğin telefonundaki bir isteme dokunursun. Sahipliğe dayalı kanıtın bir saldırgan tarafından kopyalanması daha zordur çünkü fiziksel öğeye ihtiyaç duyar.



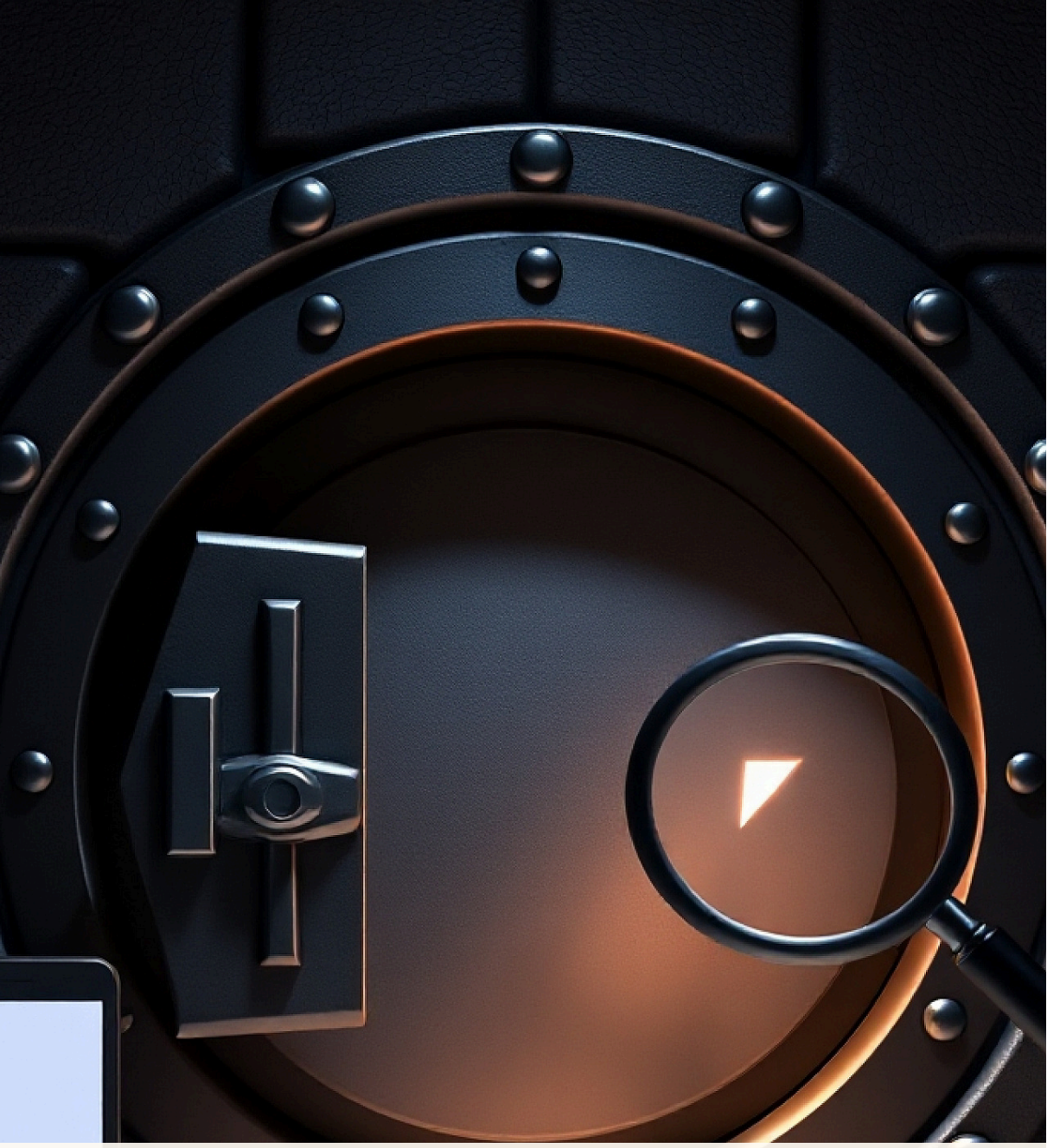
İki faktörle, yalnızca çalınmış bir parola yeterli değildir. Saldırganın ayrıca telefonun gibi ikinci öğeye de ihtiyacı olur. Bu, hesaba girmeyi çok daha zorlaştırır. Biri parolanı öğrense bile ikinci kontrol olmadan giriş yapamaz. İki faktör, yalnızca parolanın sağlamadığı bir engel ekler.



Tüm ikinci kontroller eşit derecede güçlü değildir. Bazı yöntemlerin atlatılması diğerlerinden daha kolaydır. Kısa mesajla gönderilen bir kod ele geçirilebilirken bir güvenlik anahtarının taklit edilmesi daha zordur. Yöntemin gücü önemlidir. Mümkün olduğunda daha güçlü bir ikinci faktör seç, çünkü zayıf yöntemler daha az koruma sağlar.



Hesabı gerçekten korumak için sistem doğru uygulanmalıdır. Zayıf bir kurulum faydayı ortadan kaldırabilir. Örneğin, bir ayar değiştirilerek ikinci kontrol atlanabiliyorsa koruma kaybolur. Doğru kurulum, her iki kontrolün de her zaman gerekli olması demektir. Ayrıca ikinci kontrolün bir saldırgan tarafından kolayca kapatılamaması demektir.



Hesap kurtarma seçenekleri en zayıf halka hâline gelebilir. Kurtarma kötüye kullanılmaya elverişliyse ikinci kontrol atlanabilir. Örneğin, biri tahmin edilebilir bir soruyu yanıtlayarak parolanı sıfırlayabiliyorsa ikinci faktörü atlayabilir. Kurtarma yollarının da güçlü korumaya ihtiyacı vardır. Birinin ikinci kontrol olmadan içeri girmesine izin vermemelidirler.



Yaygın bir hata, iki parolayı iki faktör olarak görmektir. Bu, bildiğin bir şey olan tek bir kanıt türünü tekrarlar. Sahip olduğun bir şey gibi ikinci bir tür eklemez. Her iki parola da öğrenilirse hesap açıktır. İki adımlı doğrulamanın faydasını görmek için aynı türden iki tane değil, iki farklı kanıt türü kullan.



Bir başka hata, girişi koruyup kurtarmayı zayıf bırakmaktır. Saldırganlar kurtarma yoluyla ikinci kontrolün etrafından dolaşabilir. Kurtarma yalnızca bulabilecekleri bilgileri istiyorsa hesabı sıfırlayıp ikinci faktörü atlayabilirler. Kurtarmayı da giriş kadar özenle güvence altına al. Aksi hâlde ikinci kontrol tamamen atlanabilir.



Bir parola artı farklı bir ikinci kontrol, girişi kırılması daha zor hâle getirir. Yalnızca parolayı bilmek her zaman yeterli değildir. Bildiğin bir şey ve sahip olduğun bir şey gibi iki farklı kanıt türü kullan. Mümkün olduğunda daha güçlü yöntemler seç. Ayrıca kurulumun doğru ve kurtarma yollarının güvenli olduğundan emin ol, çünkü bunlar korumayı zayıflatabilir.