

SIM Kart Dolandırıcılığı ile Mücadele

written by Mert SARICA | 1 March 2021

If you are looking for an English version of this article, please visit [here](#).

Günümüzde, kullandığımız e-posta hesabından sosyal medya hesabına, internet bankacılığı hesabından geliştirdiğimiz yazılımın kaynak kodunu barındırdığımız hesaba kadar giriş (login) esnasında güvenliğimiz için iki faktörlü kimlik doğrulama kullanıyoruz veya kullanmaya zorlanıyoruz. İki faktörlü kimlik doğrulama denildiğinde son yıllarda geniş kitleler tarafından sıklıkla kullanılması sebebiyle çoğumuzun aklına tek kullanımlık parola, OTP olarak SMS doğrulama kodu gelse de, tek kullanımlık parola üreten aygıtlar, uygulamalar hala hayatımızda fazlasıyla yer edinmektedir.

Yakın geçmişte yabancı basında SIM kartı değişikliği ile yapılan dolandırıcılık haberlerine sıkça rastlamaya başladık. Bu dolandırıcılıkların başarıyla ulaşmasının en büyük nedeni ise kullanıcıların doğrulama adına bir aygıt kullanmaması veya tek kullanımlık parola üreten bir aygıt, uygulama kullanmak yerine SMS doğrulama kodu kullanmalarındır. Bu sayede telefon hattını üzerine geçiren bir dolandırıcı bundan sonra bankacılıktan sosyal medya hesaplarına kadar hedef kişinin giriş esnasında cep telefonununa gönderilen tek kullanımlık SMS doğrulama kodunu ele geçirerek kötü emellerine ulaşabilmektedir. Türkiye’de bu şekilde gerçekleştirilen dolandırıcılıklar ile yıllar yıllar önce karşılaşılmaya başlandığı için bugün GSM operatörleri ile finans kurumları arasında etkin bir işbirliği yapılması ile SIM kartı değişikliği ile gerçekleştirilmeye çalışılan internet/mobil bankacılığı dolandırıcılıkları önlenebilmektedir. Son zamanlarda ise zorlu hedeflerle uğraşmak yerine kolay olanları tercih eden dolandırıcıların SIM kartı değişikliği ile kripto para borsalarında hesabı olan kullanıcıları, yatırımcıları hedef aldığını görebilmekteyiz.

Kendi hesaplarım için olabildiğince Google Authenticator gibi tek kullanımlık parola üreten uygulamalar kullansam da APT41 gibi telekomünikasyon firmalarını hedef alıp SMS meajlarına göz diken devlet destekli hacker grupları, casusa dönüşme potansiyeli git gide artan akıllı telefonlar derken telefonumu doğrulama amacıyla kullanmak bir siber güvenlik araştırmacısı olarak pek güvende hissettirmemeye başlamıştı. Bir de bağlantılarımdan “Hocam

peki sen kendi hesaplarının güvenliğini nasıl sağlıyorsun ?” vb. sorular ile de zaman içinde karşılaşmaya başladıkça bu yazı ile bilfiil hesaplarımın güvenliğini nasıl sağladığımı kısaca açıklamaya karar verdim.

SMS doğrulama koduna (something you have) kıyasla doğrulama faktörü olarak daha güvenli ne kullanabilirim diye kısa bir araştırma yaptığımda Google’ın Gelişmiş Güvenlik Programı’nda da yer alan güvenlik anahtarı üreticisi Yubico’nun web sayfasını incelemeye karar verdim. YubiKey NFC 5 anahtarını almaya karar verdikten sonra maalesef YubiKey’in bilinen e-ticaret mağazalarında satılmadığını öğrendim. Amazon.com üzerinde 45\$’a satılan bu anahtara bir o kadar da kargo bedeli üzerine bir de vergi ödememek için ne yapmalı ne etmeli diye kara kara düşünürken imdadıma o esnada FireEye etkinliği için ABD’ye uçacak olan FireEye Türkiye Kıdemli Satış Mühendisi Ökkeş ÖZDEMİR koştı ve sağolsun dertsiz, tasasız bu güvenlik anahtarına sahip olabildim.

YubiKey 5 NFC

The #1 Security Key



yubico

Anahtarı alır almaz <http://yubico.com/start> adresini ziyaret edip kurulum ile ilgili yönergeleri okuduktan sonra ilk iş olarak siber güvenlik ile ilgili haberleri takip etmek için çok sık kullandığım Twitter hesabımı güvenli hale getirmeye karar verdim. Twitter'a giriş yaptıktan sonra iki faktörlü

yetkilendirme sayfasında kısa mesaj opsiyonunu devre dışı bıraktım. Ardından güvenlik anahtarı opsiyonunu aktif hale getirip yönergeleri takip ederek USB güvenlik anahtarımı Twitter'a başarıyla tanıtarak SMS doğrulama kodu ile girişten kurtulmayı başardım. WordPress yönetim sayfasına girişte de bu anahtarı kullanabilir miyim acaba diye araştırma yaparken Two-Factor WordPress eklentisi ile de karşılaşmak beni oldukça mutlu etti.

Yeri gelmişken güvenlik anahtarı ile doğrulamayı desteklemeyen platformlar için ise Yubico tarafından geliştirilmiş olan Google Authenticator muadili, NFC destekli Yubico Authenticator uygulaması sayesinde güvenlik anahtarınızı telefonunuza NFC üzerinden okutarak tek kullanımlık parola oluşturabileceğinizi de belirtmiş olayım.



- Anasayfa
- Keşfet
- Bildirimler
- Mesajlar
- Yer İşaretleri
- Listeler
- Profil
- Daha fazla

Tweetie

Ayarlar	← İki faktörlü yetkilendirme
@MertSARICA	İki faktörlü yetkilendirme
Hesap >	Kısa mesaj ☒
Gizlilik ve güvenlik >	Cep telefonunu kullanarak, Twitter'a giriş yaptığında girmen gereken kimlik doğrulama kodunu içeren bir mesaj alabilirsin.
Bildirimler >	Kimlik doğrulama uygulaması ☒
İçerik tercihleri >	Mobil yetkilendirme uygulaması kullanarak, Twitter'a her giriş yaptığında girmen gereken bir onay kodu alabilirsin.
Genel	Güvenlik anahtarı ☐
Görünüm >	Bilgisayarına takılan veya desteklenen bir internet tarayıcısı kullanarak twitter.com'a giriş yaparken cep telefonuna senkronize olan fiziksel bir güvenlik anahtarı kullan. Şu anda Twitter uygulamasına giriş yapmak için güvenlik anahtarı kullanamazsın. Learn more
Veri kullanımı >	
Erişilebilirlik >	Ek yöntemler
Twitter Hakkında >	Yedek kodlar İki faktörlü yetkilendirme seçeneklerine erişimin yoksa, tek kullanımlık yedek kodlar alarak Twitter'a giriş yapabilirsin. >
	Geçici şifre Üçüncü taraf hizmetlerinde kullanmak için tek kullanımlık geçici şifre oluştur. >



Anasayfa

Keşfet

Bildirimler

Mesajlar

Yer İşaretleri

Listeler

Profil

Daha fazla

Tweetle

Ayarlar

@MertSARICA

Hesap

Gizlilik

Bildirimler

İçerik

Genel

Görünü

Veri kul

Erişilebi

Twitter

İki faktörlü yetkilendirme

İki faktörlü yetkilendirme

Kısa mesaj



Güvenlik anahtarı



Mert SARICA
@MertSARICA

Use a physical security key to log in to twitter.com using a supported web browser. You can either insert the key into the USB port of your computer or sync it to your mobile device over Bluetooth or NFC. [Daha fazla bilgi al](#)

We'll walk you through adding the key to your Twitter account.

Başla



Anasayfa

Keşfet

Bildirimler

Mesajlar

Yer İşaretleri

Listeler

Profil

Daha fazla

Tweetle

Ayarlar

@MertSARICA

Hesap

Gizlilik

Bildirim

İçerik

Genel

Görünü

Veri kul

Erişilebi

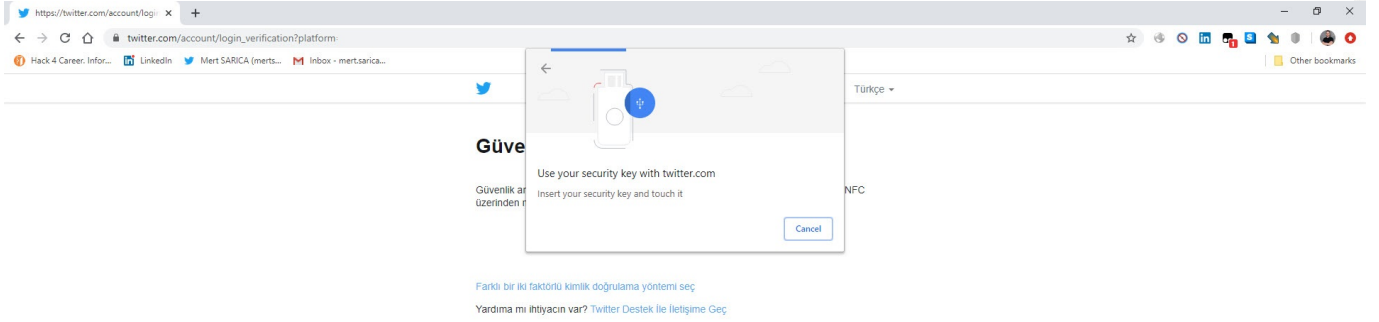
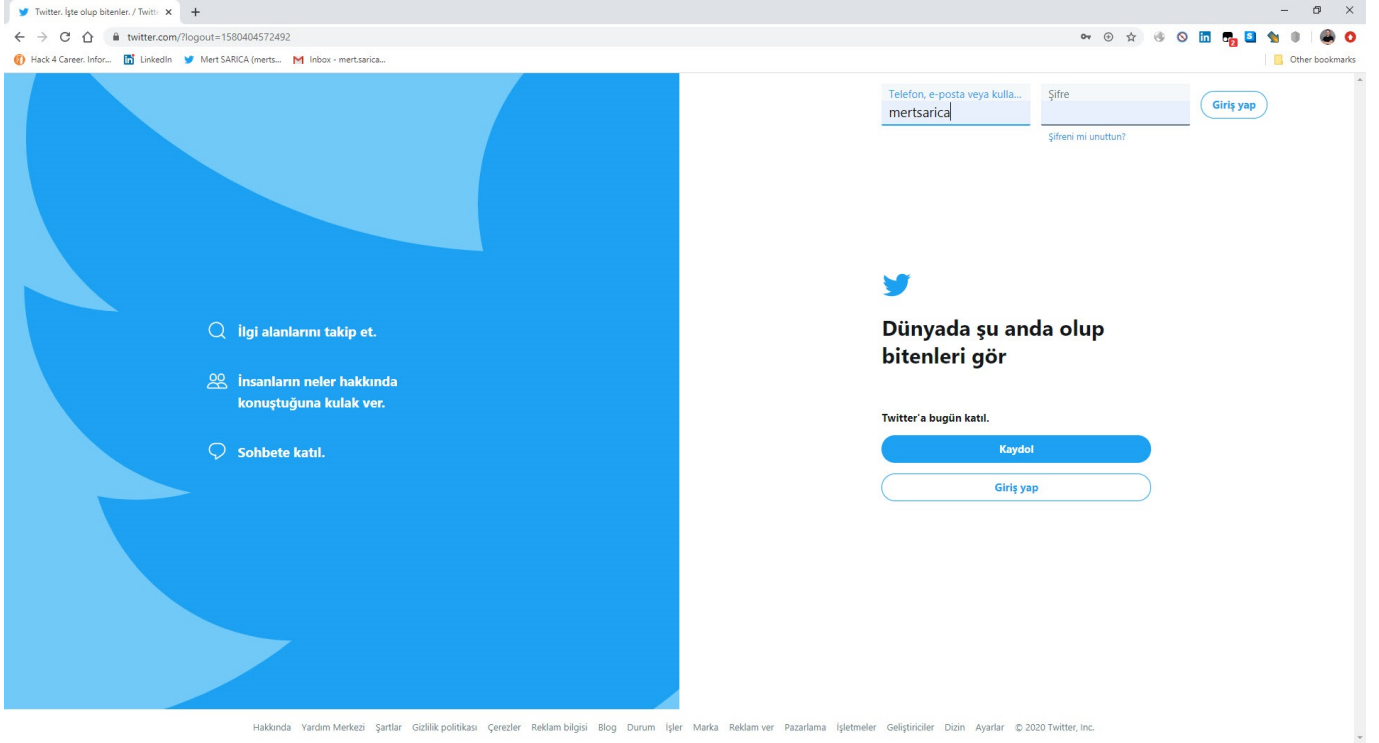
Twitter

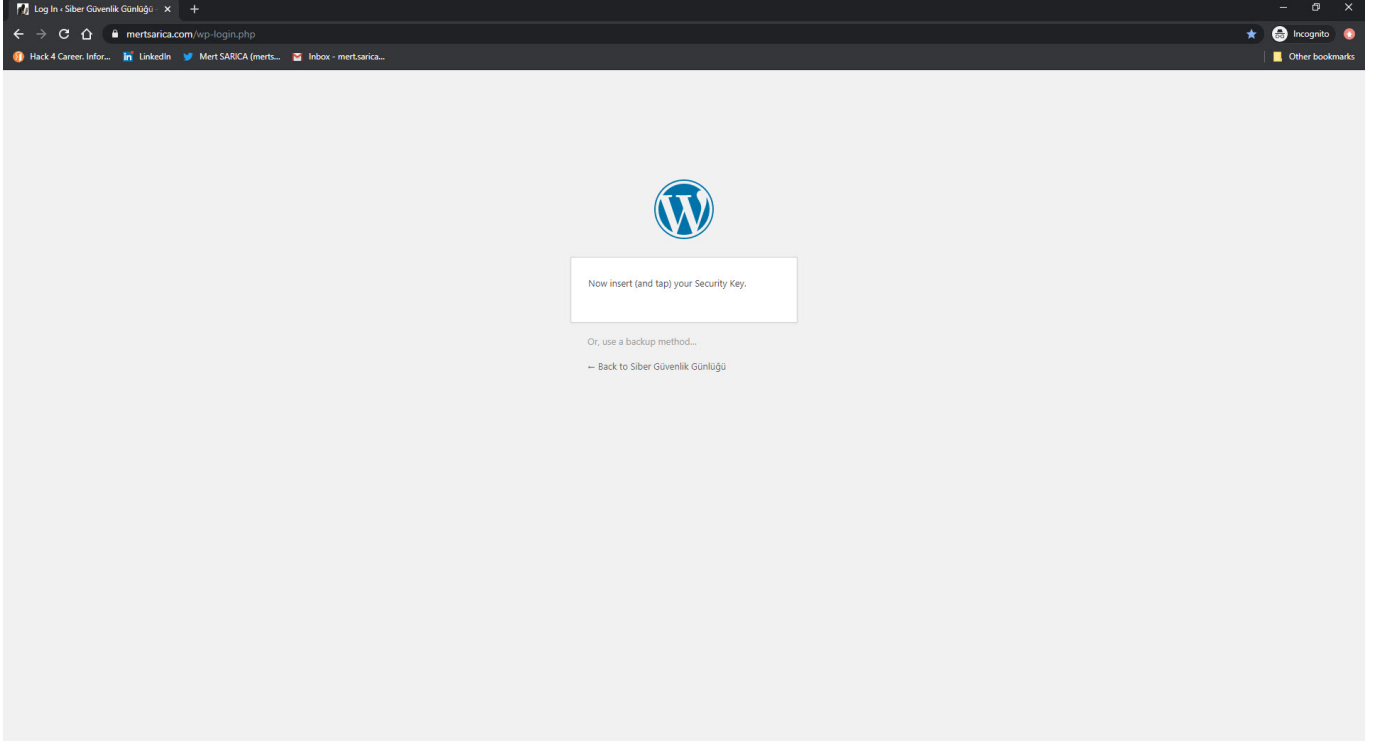


Add

Insert the security key in the USB port of your computer or sync it to your mobile device over Bluetooth or NFC, then touch the key to add it to your account.

Cancel





Son olarak Google'ın Gelişmiş Güvenlik Programı'na da dahil olup tüm Google hesaplarımı da güvenlik anahtarı destekleyen platformlarda olduğu gibi güvenli hale getirdikten sonra kendini bir nebze daha güvenli hisseden bir siber güvenlik araştırmacısı olarak mutlu sona ulaşmış oldum.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.