Combatting SIM Swapping

written by Mert SARICA | 1 March 2021

In today's world, we use two-factor authentication for security when logging in to everything from our email accounts to our social media accounts, from our internet banking accounts to the accounts that hold the source code of software we develop. When we hear the term two-factor authentication, many of us think of one-time passwords, or OTPs, sent via SMS validation codes, as they are widely used by large numbers of people in recent years. However, devices and applications that generate one-time passwords still play a significant role in our lives.

In recent times, we have frequently come across news of SIM card fraud in foreign media. The main reason for the success of these frauds is that users do not use a device for verification or use SMS verification codes instead of a device or application that generates one-time passwords. In this way, a fraudster who takes over a phone line can obtain the one-time SMS verification code sent to the target person's mobile phone during login, from banking to social media accounts, to achieve their nefarious purposes. In Turkey, as internet/mobile banking frauds attempted with SIM card changes have been encountered for many years, such frauds can be prevented through effective cooperation between GSM operators and financial institutions. Recently, instead of targeting difficult targets, we can see that fraudsters are targeting users and investors who have accounts on crypto exchanges with SIM card changes.

Even though I use one-time password generating applications like Google Authenticator for my own accounts as much as possible, with the increasing potential for smart phones to become a SPY and state-supported hacker groups like APT41 targeting telecommunication companies and SMS messages, using my phone for verification has begun to make me feel less secure as a cyber security researcher. Additionally, as I began to receive questions from my connections such as "How do you ensure the security of your own accounts?" over time, I decided to briefly explain how I ensure the security of my actual accounts with this article.

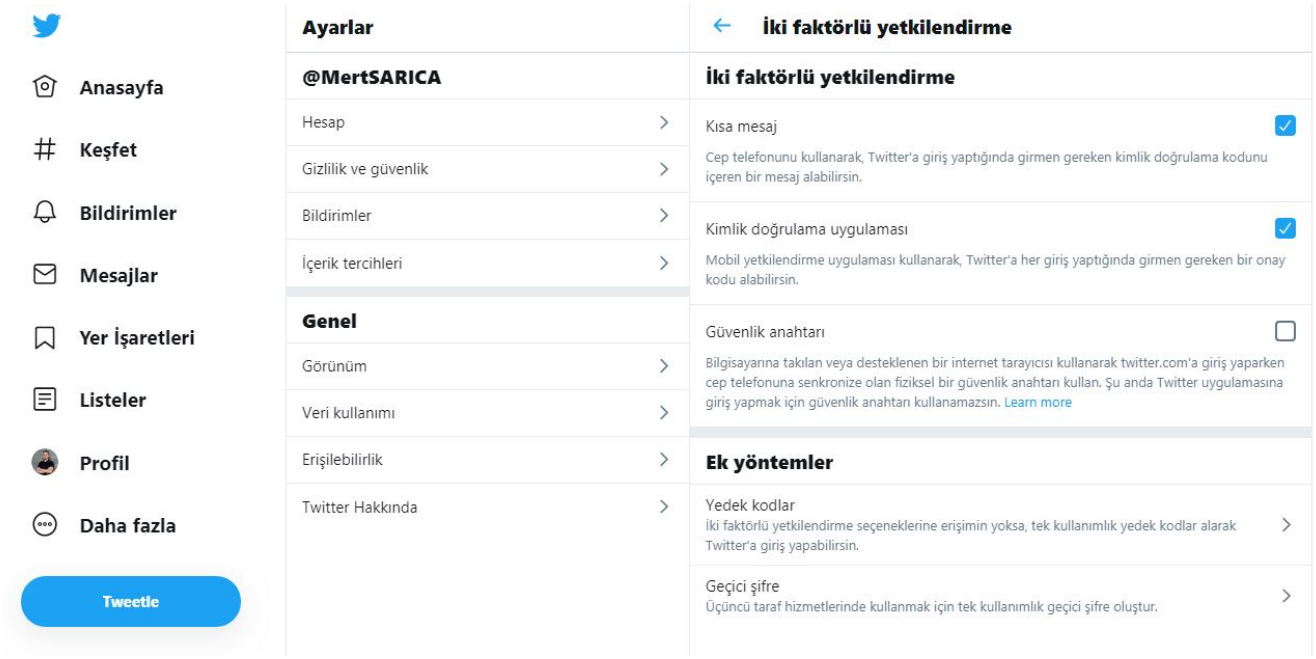
When I did a short research on what more secure verification factor I can use, instead of SMS verification code (something you have), I decided to examine the website of Yubico, a security key manufacturer that is also

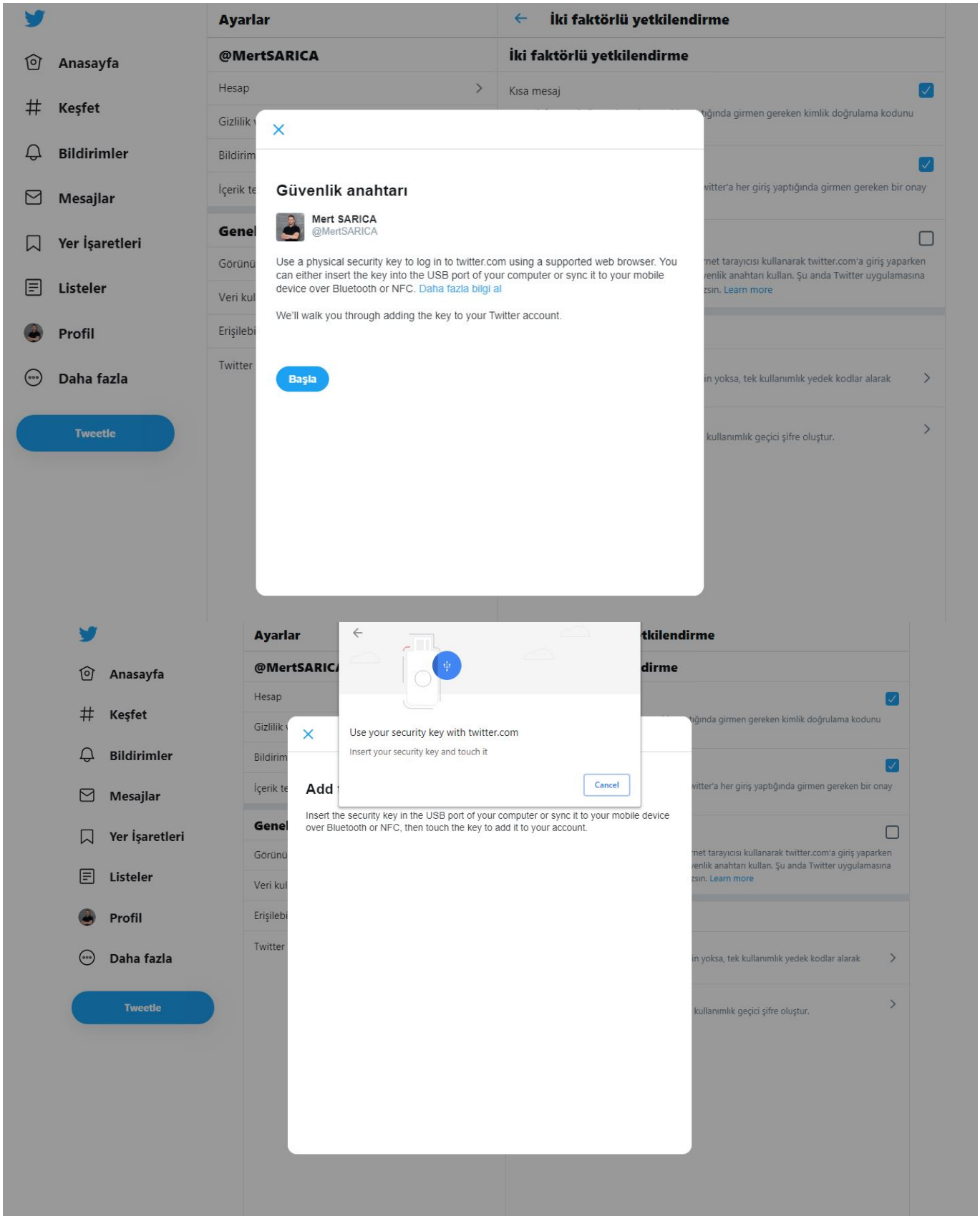
included in Google’s Advanced Protection Program. After deciding to purchase the YubiKey NFC 5 key, I unfortunately learned that it is not sold in known e-commerce stores. While I was wondering what to do to avoid paying shipping costs and taxes on top of the $45 the key is sold for on Amazon.com, my help came from Ökkeş ÖZDEMİR, Senior Sales Engineer of FireEye Turkey, who was flying to the US for a FireEye event at that time. He came to my rescue, and thanks to him, I was able to acquire this security key without any problems.

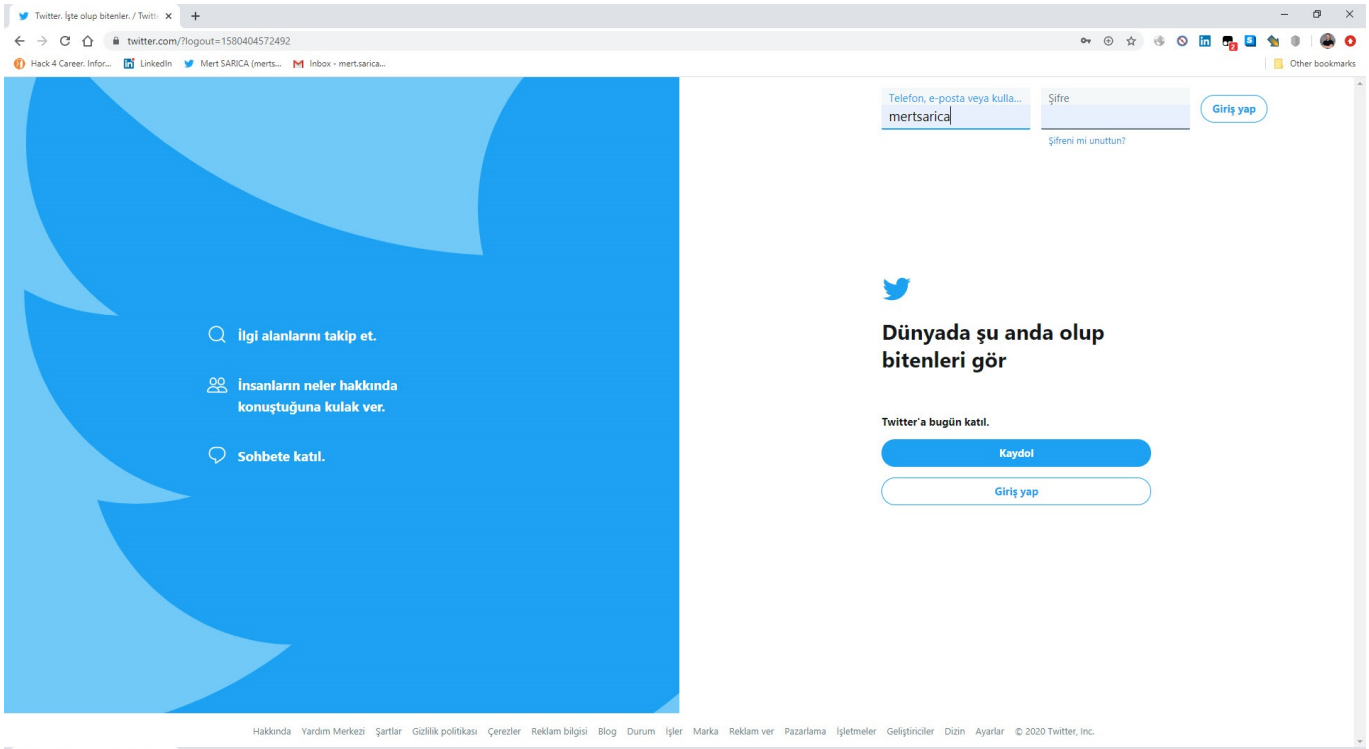
As soon as I got the key, I visited the address http://yubico.com/start and read the instructions for the setup. My first task was to make my Twitter account, which I frequently use to follow news on cyber security, more secure. After logging into Twitter, I disabled the short message option on

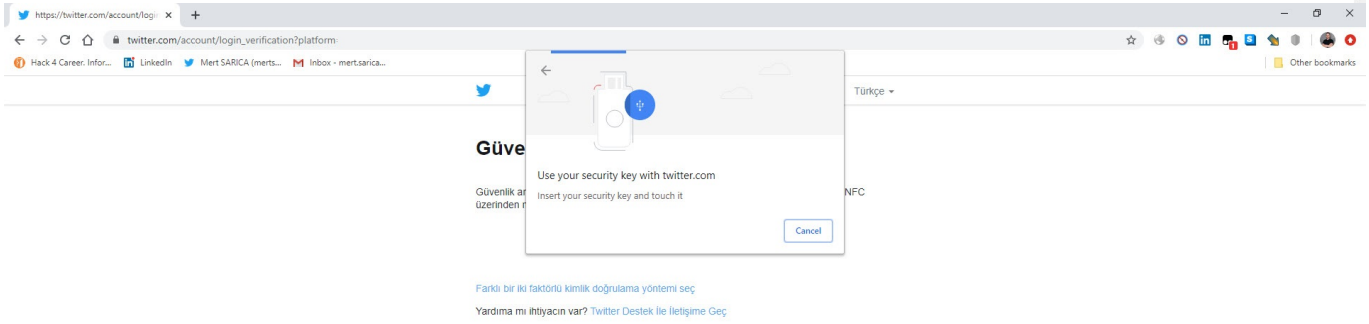
the two-factor authorization page. Then, I activated the security key option and successfully linked my USB security key to Twitter by following the instructions, thus being able to get rid of the SMS verification code during login. I also researched whether I can use this key when logging into the WordPress management page, I was happy to come across the Two-Factor WordPress plugin.

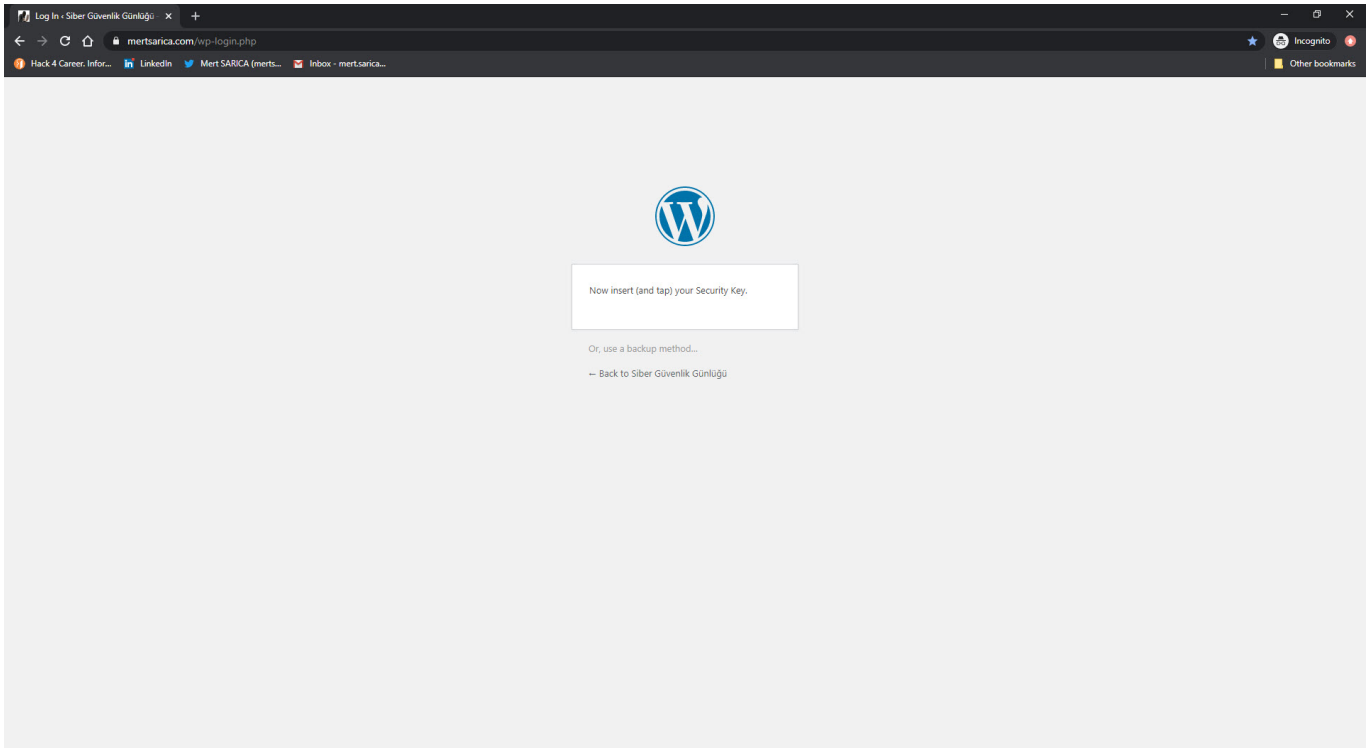
While on the subject, I should also mention that for platforms that do not support verification with a security key, Yubico has developed the Yubico Authenticator app, which is an alternative to Google Authenticator, and it supports NFC. With this app, you can create one-time passwords by scanning your security key with your phone over NFC.




Anasayfa
Keşfet
Bildirimler
Mesajlar
Yer İşaretleri
Listeler
Profil
Daha fazla
Tweetle
Ayarlar
@MertSARICA
Hesap
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
Use your security key with twitter.com
Insert your security key and touch it
Cancel
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.


Twitter. İşte olup bitenler. / Twitt
twitter.com/?logout=1580404572492
Hack 4 Career. Infor...
LinkedIn
Mert SARICA (merts...
Inbox - mert.sarica...
Other bookmarks
İlgi alanlarını takip et.
İnsanların neler hakkında konuştuğuna kulak ver.
Sohbete katıl.
Telefon, e-posta veya kulla...
mertsarica
Şifre
Giriş yap
Şifreni mi unuttun?
Dünyada şu anda olup bitenleri gör
Twitter'a bugün katıl.
Kaydol
Giriş yap
Hakkında Yardım Merkezi Şartlar Gizlilik politikası Çerezler Reklam bilgisi Blog Durum İşler Marka Reklam ver Pazarlama İşletmeler Geliştiriciler Dizin Ayarlar © 2020 Twitter, Inc.


https://twitter.com/account/logi
twitter.com/account/login_verification?platform
Hack 4 Career. Infor...
LinkedIn
Mert SARICA (merts...
Inbox - mert.sarica...
Other bookmarks
Türkçe
Güve
Use your security key with twitter.com
Insert your security key and touch it
Cancel
NFC
Farklı bir iki faktörlü kimlik doğrulama yöntemi seç
Yardıma mı ihtiyacın var? Twitter Destek İle İletişime Geç



Finally, by also joining Google's Advanced Protection Program and making all of my Google accounts secure like in platforms that support security keys, as a cyber security researcher, I feel a bit more secure and I reached a happy ending.

Hope to see you in the following articles.