Tweestapsverificatie – deel 2 –

Diensten instellen!

In het al eerder geschreven algemene verhaal over tweestapsverificatie heb je kunnen lezen wat het is, en hoe je het kunt gebruiken. In dat algemene verhaal staan de belangrijkste diensten zoals de overheid en de banken beschreven. In dit artikel vind je veelgebruikte onlinediensten beschreven. Uiteraard zijn er nog meer bedrijven die 2FA ondersteunen dan de hier genoemde. De site twofactorauth.org[1] geeft daar een uitgebreid overzicht van. Ik zal de komende weken het artikel op mijn site[2] uitbreiden met meer aanbieders van tweestapsverificatie.

Wat is het?

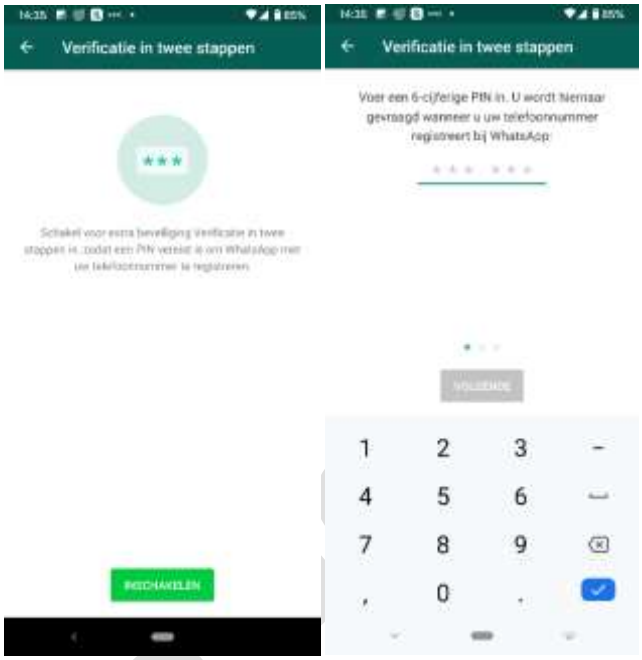
Dat is uitgebreid te lezen in het voorgaande artikel. In het kort is tweestapsverificatie een extra toevoeging aan gebruikersnaam en wachtwoord. Die extra verificatiestap doe je met een ander apparaat. Dat andere apparaat kan een telefoon zijn waarop je een code ontvangt of genereert. Het kan ook een USB-sleutel zijn of een apparaatje dat je krijgt van een instelling, of dat je moet aanschaffen. Kortom: **kennis en bezit!**

Inmiddels zijn er veel diensten die tweestapsverificatie (2FA) aanbieden. Hierna vind je een opsomming van veel gebruikte diensten. Staat een door jou gebruikte dienst er niet bij, dan kun je in het voorgaande artikel lezen hoe je dat zelf uit kunt vinden[2]. Het zou mooi zijn wanneer je het met mij zou willen delen, zodat ik dat in de opsomming kan meenemen.

WhatsApp

Inschakelen van 2FA voor Whatsapp[3] kan direct nadat je je telefoonnummer hebt geregistreerd voor WhatsApp. Je kunt dit ook later doen in je WhatsApp-account.

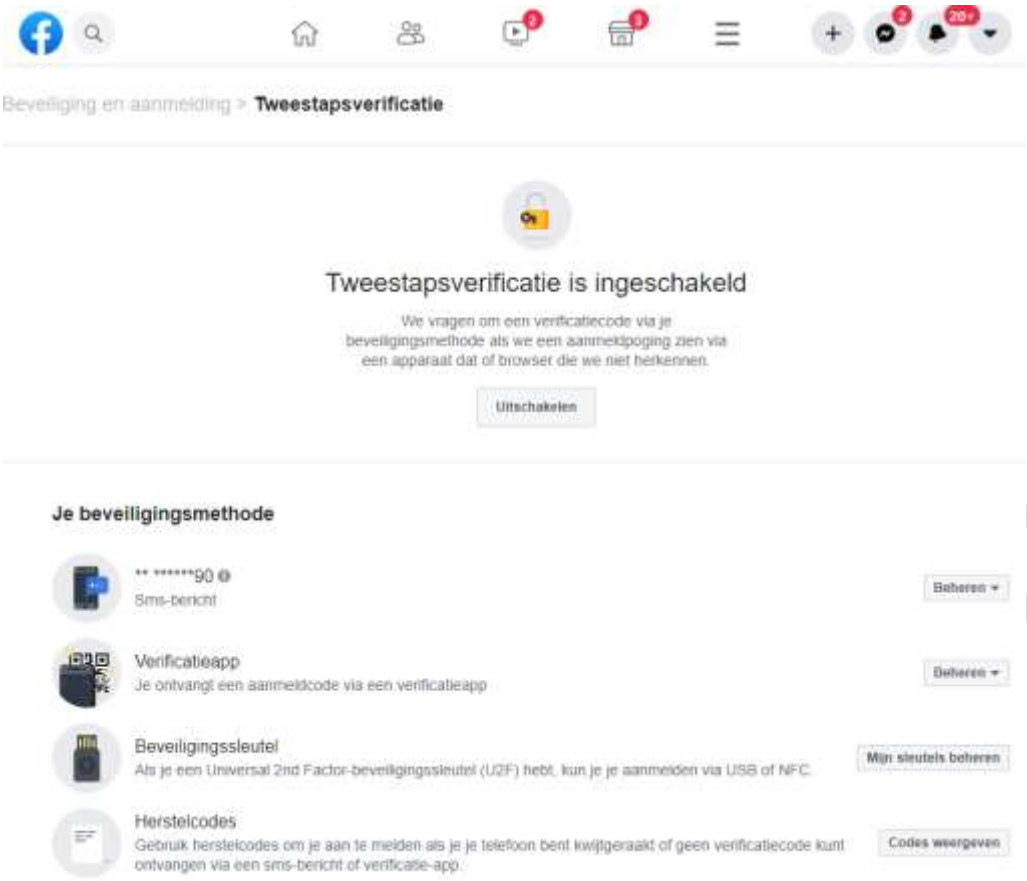
1. Open de **Instellingen** van WhatsApp.
2. Tik op **Account > Verificatie in twee stappen > Inschakelen**.
3. Voer een 6-cijferige PIN naar keuze in en bevestig deze.
4. Geef een e-mailadres op waartoe je toegang hebt of tik op **Overslaan** als je geen e-mailadres wilt toevoegen. We raden aan om wel een e-mailadres toe te voegen, zodat je je verificatie in twee stappen kunt resetten. Het helpt ook je account beter te beveiligen.
5. Tik op **Volgende**.
6. Bevestig het e-mailadres en tik op **Opslaan** of **Gereed**.



Nu is er een pincode actief waarmee je je identiteit moet bevestigen nadat je Whatsapp op een andere telefoon hebt geïnstalleerd. Zo ben je veilig voor telefoonnummerspoofing. Om niet te vergeten dat je een pincode hebt ingesteld, vraagt WhatsApp je regelmatig de pincode in te geven. Dat is vervelend, maar wel zo veilig. Je laat je huis immers ook niet onafgesloten achter. En ik vind het ook vervelend dat ik de deur steeds van het slot moet doen.

Facebook

Wanneer je 2FA voor Facebook wilt inschakelen wordt je gevraagd een keuze te maken voor een bepaalde vorm. Facebook kent, naast het zenden of creëren van een code met een generator, ook nog het gebruik van een zogenaamde Fido-sleutel[4] en herstelcodes voor nood.



Om 2FA aan te zetten voor Facebook volg je de volgende stappen:

1. Log in op je Facebookaccount en klik/tik dan op de 'pijl naar beneden' of de 'hamburger' in de rechterbovenhoek van je Facebookpagina. Klik nu op **Instellingen en privacy** > **Instellingen** > **Beveiliging en aanmelding** > **Tweestapsverificatie gebruiken.**
2. Vul daar dan in welke beveiliging je al dan niet wenst te gebruiken. Je mag er ook meerdere gebruiken. Sowieso is het wijs om de Herstelcodes te selecteren, af te drukken en op een veilige plek te bewaren.

In Facebook kun je net zoveel authenticatiemiddelen aanzetten als je wenst. Je moet tenminste het sms-bericht instellen tenzij je zowel de Verficatieapp als de Beveiligingssleutel inschakelt. Dan mag de sms-code uit.

Twitter

Wanneer je inlogverificatie voor Twitter instelt, ben je verplicht om naast de gebruikersnaam en wachtwoord ook een pincode in te voeren tenzij je een veiligheidssleutel geactiveerd hebt. Standaard is dat een 6-cijferige sms-code of je gebruikt een verificatieapp die de code voor je genereert.

Het aanzetten van de tweetrapsveiligheid doe je als volgt:

1. Klik/tik in het menu van je Twitter-account **Instellingen en privacy** eventueel voorafgegaan door een klik op het meer (…) icoon.
2. Kies nu **Beveiliging en accounttoegang** > **Beveiliging** > **tweestapsverificatie**. Dan zie je het scherm als hiernaast.

3. Heb je geen beveiligingssleutel, kies dan minimaal voor de sms-verificatie. De meeste mensen zullen voor de sms-code kiezen. Je wordt dan gevraagd je wachtwoord nogmaals in te geven, vervolgens wordt je telefoonnummer gevraagd; mocht je dat nog niet aan Twitter hebben gegeven en dan wordt een code verzonden die je vervolgens moet bevestigen.

Authy[5] gebruiken als verificatieapp.

1. Plaats een vinkje bij Verificatie-app, er verschijnt een **QR-code**.
2. Open nu **Authy** op je mobiel en klik op het menu in Authy, de **drie verticale puntjes**. Kies **Add Account** en vervolgens op **Scan QR-code**, scan deze vanaf het scherm en klik in de app op **SAVE**. De app begint nu codes de genereren; deze heb je nodig voor elke toekomstige verificatie van je Twitter-account.
3. Kies nu bij Twitter voor **[Volgende]** en er wordt een verificatiecode gevraagd. Voer daar in wat Authy genereert.

Vergeet niet de Back-upcode uit te printen en veilig op te slaan. Mocht je die niet hebben dan kan Twitter je per sms een eenmalige code zenden. Ik ben daar geen voorstander van, want dan ben je nog niet veilig voor telefoonnummerspoofing. En dat was wel de bedoeling van het gebruik van Authy en/of een veiligheidssleutel.

Authy

Op zich kun je voor Authy zelf geen tweestapsverificatie instellen, maar je kunt voor Authy op je mobiel ter beveiliging van je codes een vingerafdruk en/of pincode instellen. Doe dat! Zo beveilig je de toegang tot je verificatiesleutels. Helaas is die mogelijkheid er niet voor de Windows desktop-app.

Je stelt dat bij Authy in door in de App:

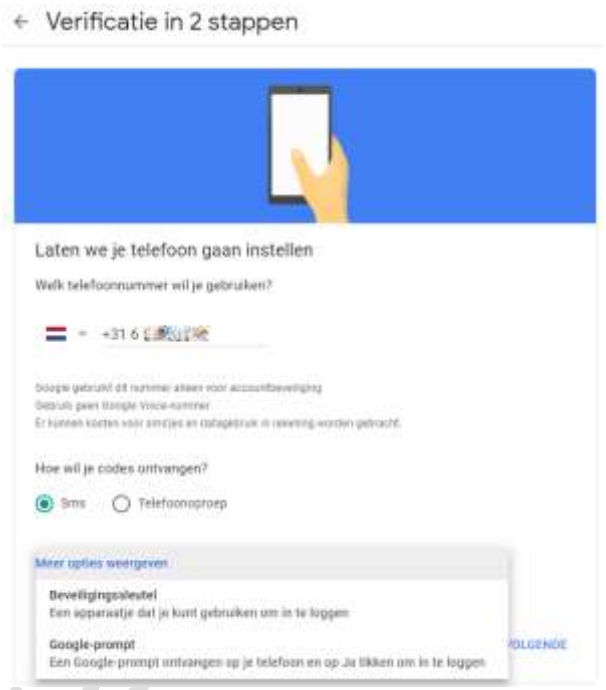
1. Op de drie horizontale puntjes te klikken
2. Kies dan onder **My Account** > **App Protection**
3. Zet daar zowel ‘Protection PIN’ alsook ‘Fingerprint’ aan

Nu is ook Authy optimaal beveiligd. O ja, vergeet ook niet om voor Authy back-ups in te stellen. Wanneer je dan een andere telefoon in gebruik neemt, kun je Authy makkelijk opnieuw instellen. Doe je dat niet, dan moet je voor elke beveiligd account de QR-codes opnieuw instellen.

Google

Google kent verschillende manieren om 2FA in te zetten. Naast je gebruikersnaam en wachtwoord wordt je dan nog om wat anders gevraagd. Dat kan een sms-verificatie of telefoonoproep zijn, maar ook een melding (prompt) op je telefoon. Wanneer je die vraag met ‘Ja’ beantwoordt, ben je binnen. Google biedt ook een beveiligingssleutel als 2FA aan, zoals een FIDO-key en de factor-authenticator-app van henzelf of Authy.

De verificatiepagina van Google bereik je door rechtsboven op je **account-icoon** te klikken en dan Beveiliging te kiezen. Blader op die pagina naar de optie: '**Verificatie in 2 stappen**'. Kies dan **[AAN DE SLAG].** Je kunt ook eerst '**meer informatie**' kiezen voor extra uitleg. Nadat je het wachtwoord nogmaals hebt verstrekt kun je *écht* aan de slag.



1. Google stelt eerst je telefoonnummer in voor sms of spraakverificatie. Welke van de twee, dat mag je zelf kiezen. Het meest gekozen is sms-verificatie. Hier kun je ook de eerder genoemde opties kiezen.
2. Google zendt je een sms of spraakoproep met een 6-cijferige code voorafgegaan door G-; je vult alleen de zes cijfers in.
3. Na de verificatie kun je op **[INSCHAKELEN]** klikken en 2FA is ingesteld.
4. Nu kom je op een pagina waar je de extra mogelijkheden kunt benutten. Vergeet vooral niet om een back-upcode af te drukken en op te slaan. Ook krijg je de mogelijkheid te zien om een back-uptelefoon in te stellen. Handig wanneer jouw eigen telefoon buiten gebruik is.

Microsoft

Microsoft is een van de weinigen die ook toestaat om, los van gebruikersnaam en wachtwoordcombinatie, in te loggen op een andere manier zoals Windows Hello of een verificatiesleutel (FIDO2). Dan heb je geen gebruikersnaam en wachtwoord nodig. Dit geldt als even veilig, zo niet veiliger dan tweestapsverificatie met gebruikersnaam en wachtwoord en een tweede factor zoals sms verificatie. In ieder geval is het makkelijker 😉

Tweestapsverificatie schakel je in door eerst in te loggen in je MS-account op de site https://account.microsoft.com/security en dan:

1. Kies Geavanceerde beveiligingsopties [**Aan de slag**]

2. Op het volgende scherm kun je Verificatie in twee stappen inschakelen. Eventueel naar beneden bladeren totdat je het vindt. Nu wordt een informatiepagina getoond. Klik op [**Volgende**].
3. Nu wordt je gevraagd om de MS-authenticator-app te downloaden. Heb je Authy of nog een andere authenticator-app, dan kun je dit overslaan. Daarvoor moet je op '**stel een andere verificator-app in'** drukken. Dan wordt een QR-code getoond die je met Authy kunt scannen en dan bevestigen. Sla je deze stap over door op [**Annuleren**] te drukken, dan gaat MS er vanuit dat je sms - of e-mail verificatie gebruikt. Je hebt immers al eerder een hersteltelefoonnummer of herstelmailadres aan Microsoft ter beschikking moeten stellen.

4. Dan wordt een herstelcode getoond. Sla deze op om te gebruiken als alle andere methoden je buitensluiten en druk af! Klik op [**Volgende**]
5. Stel een app-wachtwoord in voor je smartphone. Kies welke je wenst te maken.
   Overigens is dit onnodig wanneer je op je smartphone de app Outlook van Microsoft zelf gebruikt. Die is vanuit alle app-stores op te halen.
6. Mogelijk moet je applicatiewachtwoorden genereren voor apps en apparaten die geen 2FA ondersteunen, zoals e-mail apps Xbox 360, Mac Office 2010/2011 of eerder. Dit kan ook later. Microsoft stuurt je hierover een mail.

Je ziet aan de afbeelding dat Microsoft nog meer manieren van authenticatie kent, waarbij de beveiligingssleutel de beste optie is.

Apple

Apple's implementatie van 2FA is gebaseerd op zogenaamde 'vertrouwde apparaten'. Denk daarbij aan je iPhone, iPad of Mac. Wanneer je voor het eerst op een iApparaat inlogt wordt je, naast gebruikersnaam en wachtwoord, om een 6-cijferige code gevraagd die je óf op je telefoon óf op een al eerder vertrouwd apparaat ontvangt. Wanneer je geen 'vertrouwd apparaat' hebt, dan kent Apple geen andere mogelijkheid dan verificatie via sms- of spraakbericht.

Wanneer je inlogt met je Apple-ID op bijvoorbeeld de iCloud, en je hebt nog niet eerder 2FA ingesteld, dan dwingt Apple dat af. Log je in met je Apple-ID in de iCloud, dan krijg je het scherm hiernaast. Ga je door, dan kan het zijn dat je extra veiligheidsvragen voorgeschoteld krijgt. Vragen die je zelf al eerder had ingesteld. Hierna wordt je verzocht een telefoonnummer voor sms-verificatie of een gesproken oproep in te voeren als je dat al niet hebt gedaan.

Omdat Apple 2FA afdwingt, kun je het niet uitschakelen.

PayPal

PayPal biedt al heel lang 2FA gebaseerd op een sms-code. En omdat gebruikers ook nog betere beveiliging wensen, is daar nu ook 2FA op basis van een door een authenticator gegenereerde code aan toegevoegd.

Je stelt 2FA op PayPal in door op je account in te loggen en dan Instellingen (het tandwiel) te kiezen.

1. Vervolgens klik je op 'VEILIGHEID'.
2. Achter tweestapsverificatie kies je 'Instellen'
3. Nu kun je een keuze maken welke 2FA-vorm je wenst; sms of een authenticator-app

PayPal kent geen back-upcodes; het is verstandig om naast Authy als authenticator-app ook een sms-code in te stellen. Het is wijs om dat op een andere telefoon in te stellen dan de normaal door jou gebruikte telefoon.

LinkedIn

Twee methodes worden door LinkedIn ondersteund. De al bekende SMS-verificatie en daarnaast met een gegenereerde code van een verificatie-app. LinkedIn noemt het dubbele verificatie.

Er is verschil bij het instellen op een computer of op een mobiel apparaat.

Instellen op de desktop is verreweg het makkelijkst:

1. Klik bovenaan op de LinkedIn pagina op je '**ik-picto**' > '**instellingen en privacy**'
2. Selecteer in de volgende pagina: '**Aanmelding en beveiliging'** en klik op '**Wijzigen**' achter '**Dubbele verificatie**'
3. Schakel daar de dubbele verificatie in en kies welke methode je wenst en klik op [**Doorgaan**]. Nu wordt uit veiligheid nogmaals je wachtwoord gevraagd.
4. Heb je zoals aanbevolen voor een authenticator-app gekozen, dan wordt de QR-code getoond die je met Authy kunt scannen en vervolgens bevestigen.

Inschakelen met een mobiel apparaat:

1. Tik ook hier op je **profielfoto** > **Instellingen** > **Aanmelding en beveiliging**
2. Verder gaat het vergelijkbaar zoals op de desktop alleen kun je nu geen QR-code scannen. Je zult je de beveiligingssleutel moeten kopiëren en plakken in Authy of een andere verificator-app.

Dropbox

Dropbox kent net als de meeste diensten maar twee manieren om 2FA in te zetten. Naast je gebruikersnaam en wachtwoord wordt je dan nog om wat anders gevraagd; een sms-verificatie of

een gegenereerde code op een verificatie-app. Tweestapsverificatie kun je alleen in de browser instellen. Ga daarvoor naar dropbox.com en log in met je gegevens.

Je stelt 2FA dan als volgt in:

1. Klik op de **accountafbeelding** > **Instellingen**
2. Tabblad '**Beveiliging**'
3. Tweestapsverificatie inschakelen (Nogmaals je wachtwoord invoeren)
   Dan kiezen voor een van de twee mogelijkheden.
4. Scan de QR-code en bevestig deze
5. Vergeet niet de back-upcodes te noteren en veilig op te slaan

Nu je toch bij de veiligheidsinstellingen van Dropbox bent is het een mooie gelegenheid om ook de beveiligingscontrole van Dropbox te doorlopen.

Amazon

Als grote speler heeft Amazon uiteraard tweestapsverificatie als beveiliging opgenomen. Amazon noemt dat OTP (One Time Password). Het valt me wel tegen dat Amazon alleen sms en een verificatie-app ondersteunt en geen FIDO-sleutel.

Instellen van 2FA:

1. Log in op amazon.nl. Klik dan op bovenin op **je naam** > **account**
2. Kies daar voor **'Aanmelden en beveiliging'**
3. Nu op [**Bewerken**] klikken achter '*Instellingen voor verificatie in twee stappen (2SV):*'
4. Kies nu een van de twee methodes.
5. Bevestig de keuze door de terugmeldingscode in te geven

LastPass

LastPass is een goede wachtwoordmanager die al de wachtwoorden versleuteld op zijn server opslaat. Ontsleutelen van de wachtwoorden gebeurt lokaal op je eigen computer of mobiel apparaat. Voor gebruikers die voor LastPass betalen biedt het ook ondersteuning voor YubiKey en vingerafdruklezers. Gebruikt je LastPass gratis, dan is het 'behelpen' met een authenticator-app, sms-codes via DUO of een tabel (grid) met codes.

Het beheren van tweestapsverificatie doe je in de browser:

1. Klik op je **account** rechtsboven in de browser > **accountinstellingen**
2. Kies dan: **'Opties voor meervoudige verificatie'**
3. De meeste mensen zullen hier voor een verificatie-app kiezen (LastPass of Google Authenticator). Heb je een andere authenticator-app, kies dan de 'Google authenticator' voor de te doorlopen stappen. Deze zijn voor andere authenticator-apps zoals Authy of de Microsoft-authenticator gelijk.

Tot slot

Kijk op mijn site en zoek dit artikel[2]. In de loop der tijd worden er meer diensten waar je 2FA kunt gebruiken toegevoegd. Roept u maar!

Links:

1. 2FA ondersteuning https://bit.ly/r-tfa
2. Dit artikel – groeiend - https://bit.ly/r-mfa
3. WhatsApp https://bit.ly/r-wap
4. Fido2-sleutel https://bit.ly/r-fido2
5. Authy https://bit.ly/r-hndla
6. Mijn andere artikelen https://bit.ly/r-art