Tweestapsverificatie

Wat is het en waarom moet je het gebruiken?

Omdat de altijd online-wereld steeds onveiliger wordt, is het noodzaak jezelf beter te beveiligen en met meer beveiligingsmiddelen dan alleen de niet meer zo veilige, maar vertrouwde gebruikersnaam/wachtwoordcombinatie. Dat heeft geleid tot de ontwikkeling van tweestapsverificatie, of zoals de Amerikanen zeggen: Two Factor Authentication (kortweg: 2FA).

Inloggen met een gebruikersnaam en wachtwoordcombinatie is met de jaren steeds minder veilig geworden. Door betere en snellere computers is het makkelijker geworden om met brute kracht een wachtwoord te kraken. Vooral wanneer je, net als veel gebruikers, voor elke inlog eenzelfde combinatie van gebruikersnaam en wachtwoord gebruikt. Zo maak je het immers voor hackers wel erg makkelijk. Wanneer ze eenmaal die combinatie van je hebben gevonden, krijgen ze toegang tot al de accounts die op dezelfde manier beveiligd zijn. Laat staan dat ze ook op de hoogte zijn van veiligheidslekken waar we dagelijks van horen en waardoor miljoenen combinaties van gebruikersnaam en wachtwoorden op straat komen te liggen.

Vanwege dit probleem bieden veel organisaties, websites en computerfabrikanten en producenten van mobiele apparaten de mogelijkheid om via tweestapsverificatie in te loggen. Banken zijn daar als eerste mee begonnen door te vereisen dat je alleen toegang tot je bankrekening kunt krijgen op basis van kennis en bezit. In dit geval je pincode, pinpas en de zogenaamde authenticator.

Ik probeer hier uit te leggen wat tweestapsverificatie (2FA) precies inhoudt; hoe het werkt en de manier waarop het bijdraagt aan een veiligere manier van authenticatie, wat de hindernissen zijn en waarom je het zou moeten gebruiken. Het beschrijft ook aanbieders van diensten die tweestapsverificatie gebruiken ter bescherming van de aanmelding en de gegevens die je aan hen toevertrouwt.

Wat is tweestapsverificatie

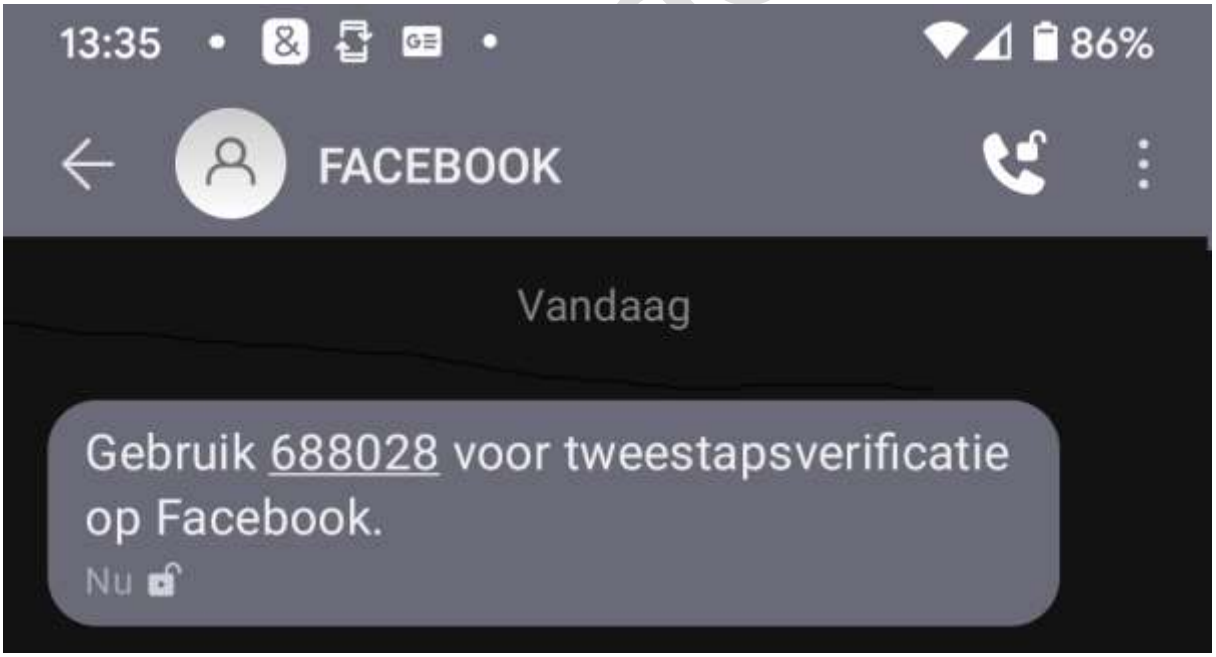
Tweestapsverificatie (2FA), ook wel Multi Factor Authenticatie (MFA) genoemd is een inlogmethode die wordt gekenmerkt door het vereisen van twee sleuteldelen. Vaak behelst het kennis van een code en het bezit/gebruik van een geregistreerd apparaat waarmee het tweede codedeel wordt ontvangen of gegenereerd. Dus naast de gebruikersnaam/wachtwoordcombinatie is er dan nog een sleuteldeel (code) nodig ter bevestiging van je identiteit.

De meest bekende vorm van tweestapsverificatie is bij de bank waar je zowel je pinpas als je pincode nodig hebt om geld uit de muur te trekken of te betalen bij een pinautomaat. Daarnaast kennen de meeste banken ook Multi Factor Authenticatie wanneer je geld overmaakt. Dan wordt naast de pinpas/pincode/vingerafdruk-inlog ook nog verwacht dat je met een authenticator een code genereert die je vervolgens moet invoeren.

Tweestapsverificatie kan uit verschilde extra componenten bestaan. Eén daarvan als bijna altijd een gebruikersnaam/wachtwoordcombinatie aangevuld met het bezit en benutten van een apparaat. De implementatie verschilt van organisatie tot organisatie. Elk van de methoden heeft zijn eigen voor en nadelen. Het grootste nadeel is voor iedereen: ‘het gedoe’. Het kost meer inspanning om veilig te werken en dat extra werk willen we eigenlijk niet.

Tweestapsverificatie op een mobiel apparaat

Je kunt als tweede factor je mobiel gebruiken. De betreffende website of dienst stuurt je een sms met een code die je ter verificatie moet invoeren. Ook kun je op je mobiel een bericht krijgen dat je met Ja of Nee dient te beantwoorden of je moet een speciale app starten om de code te generen.



In het voorbeeld hierboven maakt Facebook gebruik van een tweede factor door mij een SMS te zenden. Je hebt dus al je gebruikersnaam en wachtwoord ingevuld en de eenmalige, beperkt geldige, code vul je in zoals gegenereerd of ontvangen op je mobiel. Een ander voorbeeld is DigiD met SMS-verificatie.

Voordelen:

- Het is gebruikersvriendelijk
- Je hoeft geen authenticator mee te nemen omdat het proces gebruik maakt van je eigen mobiele apparaat
- De codes worden op aanvraag aangemaakt en zijn maar een beperkte tijd geldig, en daardoor veiliger dan statische wachtwoorden.
- Er is een beperkt aantal pogingen toegestaan waardoor het risico op kraken wordt verkleind.

Nadelen:

- Ben je buiten het bereik van het GSM-netwerk, dan bereikt de code je niet
- Je mobiel kan gestolen, verloren of beschadigd zijn
- Hackers kunnen via SIM-kloning toegang krijgen tot de sms-code (Spoofing)
- Door je mobiele nummer te delen met de betreffende dienst geef je privacy prijs.

Bovengenoemde nadelen kunnen worden voorkomen door een authenticator-app te gebruiken. Een auhenticator-app genereert codes die je als tweede factor kunt invoeren bij een daarvoor geschikte dienst. Het meest bekend is de Google-authenticator, die ik niet vertrouw omdat het geen OpenSource is. Ik gebruik liever Authy[1] als authenticator-app. Je koppelt de dienst aan Authy door bij de dienst een QR-code te scannen en ter verificatie de gegenereerde code te retourneren. Authy genereert de code die door de bewuste dienst als tweede factor wordt gevraagd.
Van Authy zijn naast de mobiele uitvoeringen ook versies voor op de desktop. Authy kan van de door jou geactiveerde diensten back-ups maken die gekoppeld zijn aan jouw telefoonnummer en een wachtwoord. Het voert te ver om verder over Authy uit te weiden; misschien iets voor een toekomstig artikel. Zo moeilijk is het niet. Een kwestie van goed lezen en wanneer je de Engelse taal niet machtig bent is DeepL[2] je beste vriend om je bij het vertalen bij te staan.

2FA met Random reader/-scanner/Digipas

Andere bedrijven, waaronder veel banken, leveren kastjes waarmee je een code kunt genereren of waar continu wisselende code op wordt getoond. In het eerste geval voer je je pinpas (niet bij de Digipas) en pincode in, waarna eerst een nummer moet worden ingevoerd of een plaatje van het scherm moet worden gelezen. Vervolgens wordt een sleutel getoond die op het scherm ingevoerd moet worden.

De door de banken gebruikte methode kan ook gebruikt worden om in te loggen bij bedrijven en instellingen die iDIN[3] gebruiken. iDIN is een dienst van de banken om je, met veilige en vertrouwde middelen van de eigen bank, te identificeren.

Voordelen:

- Makkelijk in gebruik
- Geen mobieltje nodig
- Het kan simpel meegenomen worden
- Random readers zijn uitwisselbaar.
- De code verandert periodiek; waardoor er geen wachtwoord te stelen is.

Nadelen:

- Het is vatbaar voor man-in-the-middle[4] aanvallen
- Apart extra apparaat om mee te nemen.

2FA met Veiligheidssleutels

Met veiligheidssleutels worden fysieke Fido-sleutels[5] bedoeld; het zijn speciale kleine USB-sleutels, die je aan een sleutelbos kunt hangen. Daarmee bescherm je je accounts. De Fido-sleutel _*ís*_ de tweede factor. Sommige van de sleutels staan je ook toe om mail te versleutelen en er zijn er ook die naast het gebruik van de sleutel je vingerafdruk scannen en verifiëren. Je kunt de sleutel zelf nog extra te beveiligen met een pincode zodat hij onbruikbaar is bij verlies of diefstal. De dienst zelf krijg nooit jouw pincode of vingerafdruk doorgegeven. Een Fido-sleutel is het veiligste tweestapsverificatie middel dat er is en kan een gebruikersnaam/wachtwoordcombinatie overbodig maken. Lees meer in het online artikel van c't[3]. Dat bracht mij ertoe om er zelf een aan te schaffen. Ik gebruik de Yubikey 5 nano. Inmiddels zijn er ook keys met NFC-chip voor mobiel gebruik. Daar zou ik nu voor gaan.

Voordelen:

- Makkelijk in gebruik; een druk op de knop of vingerscan is voldoende
- Geen mobieltje nodig; geen telefoonnummer te delen
- Het kan erg makkelijk worden meegenomen
- De code verandert periodiek; waardoor er geen wachtwoord te stelen is.

Nadelen:

- Je moet je Fido-sleutel altijd op zak hebben of daarnaast nog een tweestapsverificatie voor de dienst instellen.
- Het kost geld om er een aan te schaffen. Maar wat is een paar tientjes voor extra veiligheid?!?

Diensten die tweestapsverificatie gebruiken

We kijken hier naar een aantal van de meest voorkomende instellingen en bedrijven die tweestapsverificatie gebruiken om de identiteit van gebruikers te verifiëren wanneer ze inloggen. De meeste diensten verplichten het gebruik van 2FA (nog) niet. Dat zouden ze naar mijn mening wel moeten doen!

We gaan kijken hoe de overheid, Facebook, Twitter, Google, Apple, Microsoft en Paypal gebruik maken van 2FA. Ze gebruiken 2FA allemaal op een iets andere manier. Voor elk van deze instanties bekijken we hoe je 2FA instelt en hoe het bij inloggen werkt.

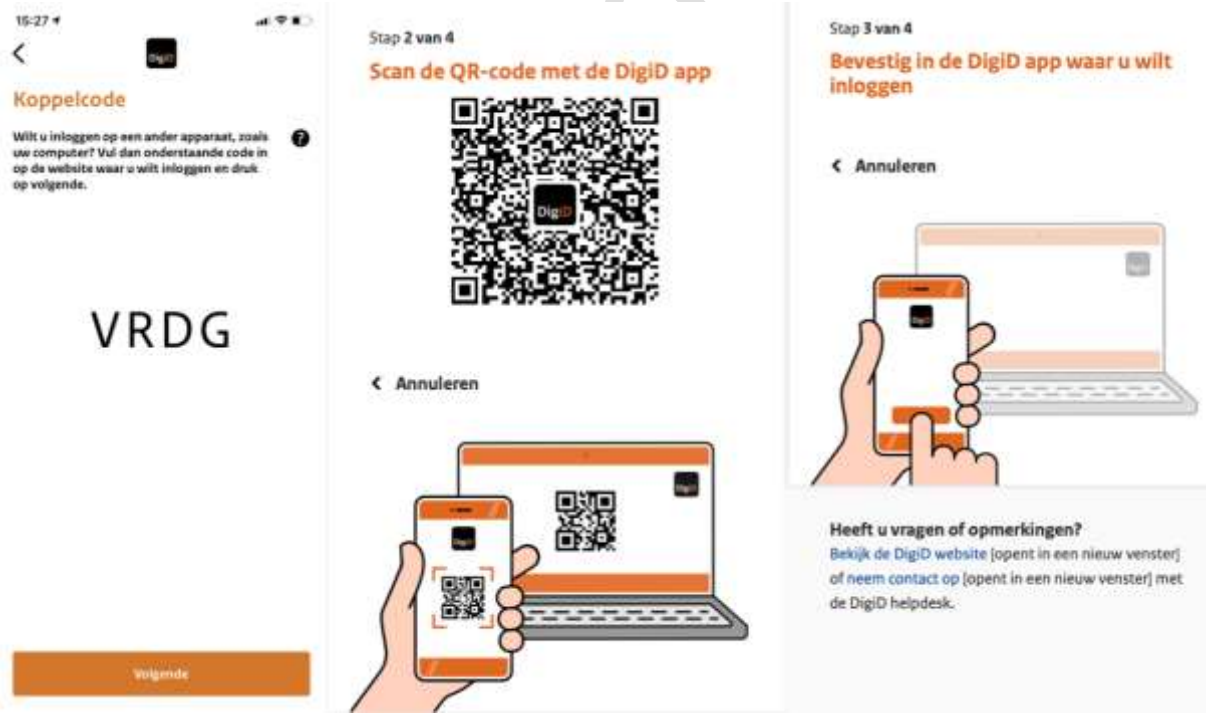
De overheid

De overheid heeft de DigiD[6] ingesteld om je eenduidig te kunnen identificeren bij instellingen die wettelijk bevoegd zijn om Burgerservicenummers (BSN) te gebruiken, zoals overheidsinstellingen,

pensioenfondsen, het onderwijs, de zorg en zorgverzekeraars. Iedere ander bedrijf of organisatie mag dus nooit, maar dan ook nooit, uw BSN vragen, laat staan opslaan!
Met de DigiD toon je wie je bent wanneer je via internet iets regelt en je gegevens blijven goed beschermd. DigiD is te gebruiken met alleen een gebruikersnaam en wachtwoord, dat moet je echter niet willen. De makkelijkste manier om in te loggen is met de DigiD app en wil, of kun je dat niet, log dan in met sms-controle. Wanneer je extra privacygevoelige zaken met je DigiD wilt inzien of wijzigen dan is een extra controle van een identiteitsbewijs nodig. De ID-check kan door de app eenvoudig worden gedaan wanneer je mobiel de NFC-code van je ID kan lezen. Lukt dat niet, dan kun je iemand anders vragen dat voor je te doen wanneer die bereid is om via de CheckID-app voor jou de ID-check uit te voeren.

Wil je digitaal zaken doen met de overheid, dan is gebruik van een DigiD verplicht. Je vraagt deze aan en activeert die op de site van digid.nl. Nadat je je BSN, geboortedatum, postcode en huisnummer hebt ingevuld, kun je een gebruiksnaam en wachtwoord kiezen. Het is wijs om dan meteen je mobiele nummer voor een sms-controle op te geven. Heb je geen mobiel nummer, dan is een vast nummer ook een optie om een gesproken sms te kunnen ontvangen. Dan rest nog het invullen van een e-mailadres. Er vinden nog wat controles plaats. Vervolgens krijg je een brief thuisgestuurd met de activatiecode.
Wanneer alles is afgerond activeer dan voor je eigen veiligheid de DigiD-app.

Ik kan hier precies alle stappen uitleggen, maar op digid.nl staan uitstekende stappenplannen voor het veilig werken met je DigiD. Om er verzekerd van te zijn dat 2FA altijd voor jouw DigiD inlog wordt gebruikt, moet je dat natuurlijk wel instellen door in te loggen op mijn.digid.nl en daar de instelling aan te passen.

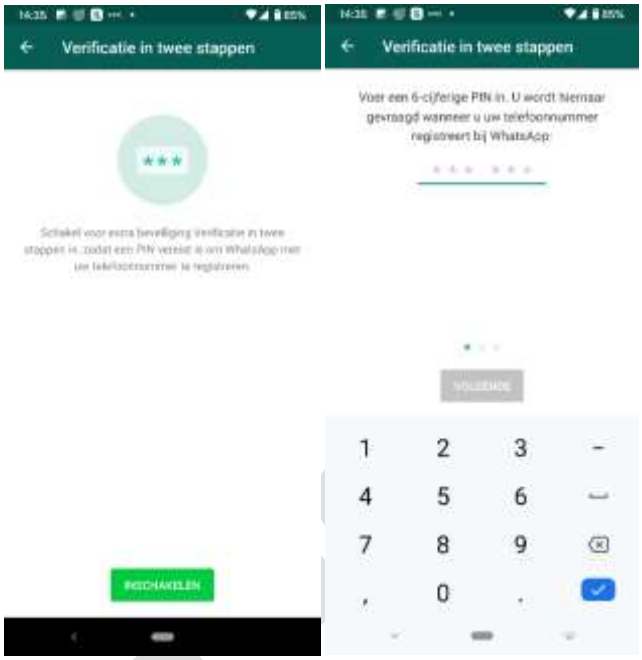


Wil je inloggen op een website met je DigiD, dan heb je de keus uit inloggen met sms-code of de app. Kies je voor de app, dan open je die en vul je na op [**Start**] gedrukt te hebben de koppelcode in, vervolgens scan je de getoonde QR-code en nadat je je eigen pincode hebt ingevuld, krijg je toegang.

WhatsApp

Inschakelen van 2FA voor Whatsapp[7] kan direct nadat je je telefoonnummer hebt geregistreerd voor WhatsApp. Je kunt dit ook later doen in je WhatsApp-account.

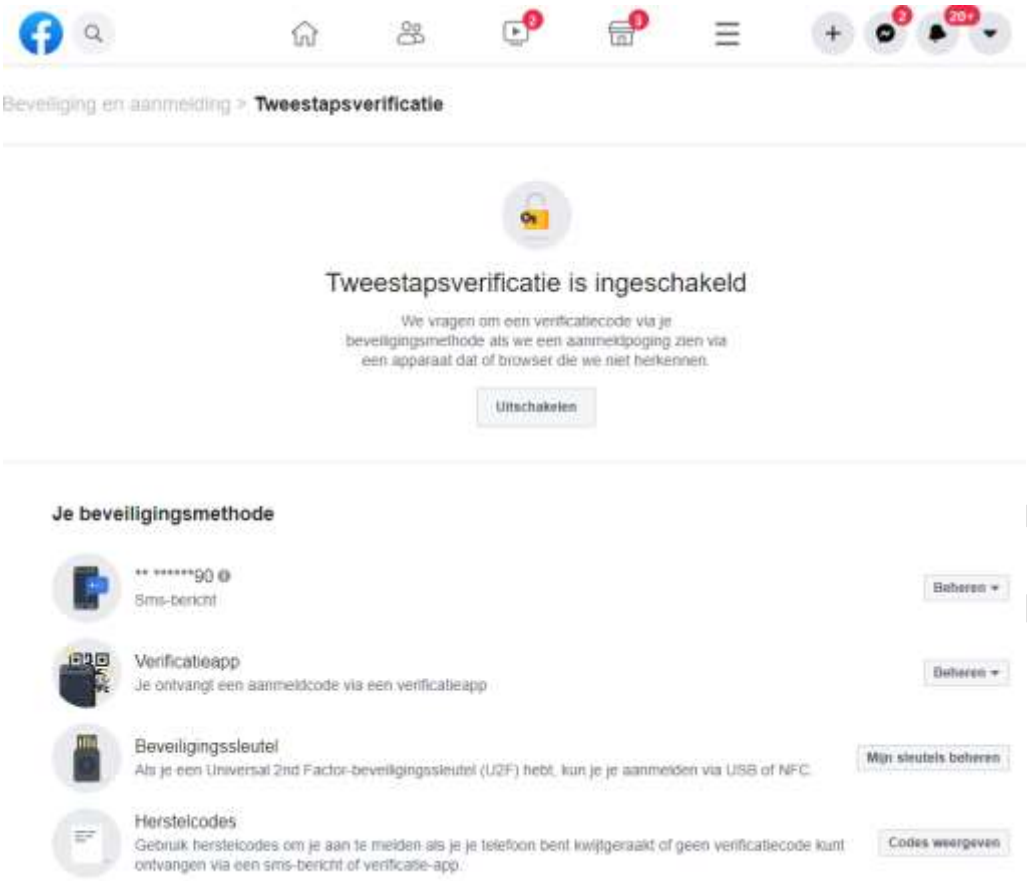
1. Open de **Instellingen** van WhatsApp.
2. Tik op **Account > Verificatie in twee stappen > Inschakelen**.
3. Voer een 6-cijferige PIN naar keuze in en bevestig deze.
4. Geef een e-mailadres op waartoe je toegang hebt of tik op **Overslaan** als je geen e-mailadres wilt toevoegen. We raden aan om wel 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 gevaagd 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[3] en Herstelcodes voor nood.



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

1. Log in op je facebook account 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 gebruiken als verificatieapp.

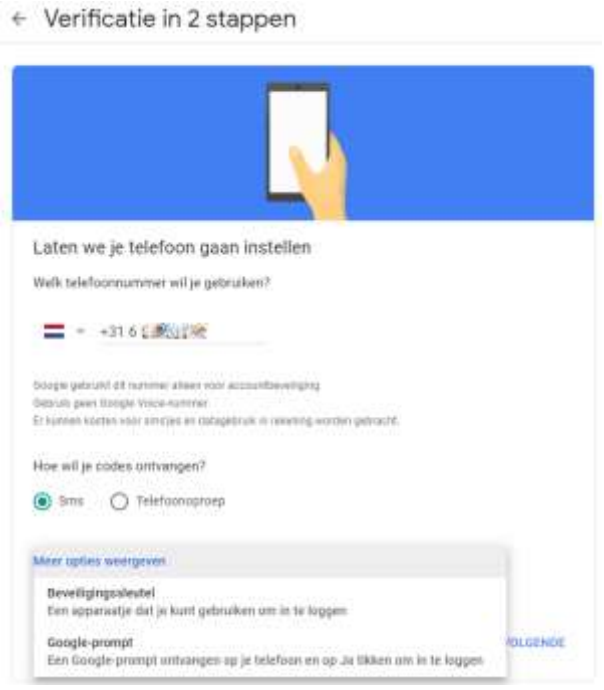
1. Plaats een vinkje bij Verificatie-app, er verschijnt een **QR-code**.
2. Open nu **Authy** op je mobiel en klik op het menu in Authy, de **drie verticale puntjes**. Kies **Add Account** en vervolgens op **Scan QR-code**, scan deze vanaf het scherm en klik in de app op **SAVE**. De app begint nu codes 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.

Google

Google kent ook 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 beantwoord, 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 rechts boven 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 het 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 verplicht veiligheidsvragen te beantwoorden krijgt die je ooit hebt 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.

En groeiend

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

Bij het uitkomen van het blad zijn daar sowieso diensten aan toegevoegd, waaronder:

- Authy
- Paypal
- LinkedIn
- Signal
- Telegram
- LastPass
- 1Password
- BackBlaze
- DropBox
- Evernote
- Amazon

Zelf uitvinden of een site 2FA ondersteund

Hoewel hier veel financiële, sociale en opslag-diensten zijn behandeld die 2FA aanbieden, zijn er veel websites gekoppeld aan andere aanbieders die mogelijk ook 2FA-bescherming bieden. Log in bij de dienst waarvan je dat wilt onderzoeken; ga dan naar **'Instellingen'** en kijk of er bij je profiel een onderdeel '**beveiliging'** of' **wachtwoorden'** is. Mogelijk vind je daar 2FA en kijk anders in de FAQ of het forum van de dienst. Vaak kan een simpele zoekopdracht in een zoekmachine waardevolle informatie opleveren.

Mocht je zelf nog belangrijke diensten bedenken, meld mij die dan. Ook graag een melding wanneer een van de diensten zijn methodiek heeft gewijzigd waardoor de beschrijving niet meer klopt.

Mochten er sites zijn waarbij je verbaasd bent dat 2FA niet ondersteund wordt zoals Xs4all en KPN, bestook dan de helpdesk met de prangende vraag waarom zij zo lichtvoetig met hun gebruikersgegevens omgaan en dring er op aan dat dit alsnog wordt geactiveerd.

Wat moet je nog meer weten over tweestapsverificatie ?

Aangezien je mail-accounts de **'belangrijkste accounts'** zijn die je hebt, is elk mail account uiteraard beveiligd met 2FA!. Denk er maar eens aan hoeveel diensten jou de afgelopen jaren naar je e-mailadres hebben gevraagd. Het zal je duizelen! Ook al gebruik je het mailadres niet om in te loggen, het wordt wel gebruikt als herstelmailadres!

Je moet daarom je mailaccounts TOP-beveiligen met een lang, en dan bedoel ik ook LANG en uniek wachtwoord. Op het moment van schrijven (2021) minimaal vijftien tekens, maar liever nog langer om een brute kracht aanval te kunnen weerstaan.

Hackers kunnen je heel veel schade en ongemak berokkenen wanneer zij de toegang krijgen tot je mailaccount. Met tweestapsverificatie , en een oplettende gebruiker wordt dat bijna onmogelijk!

Je moet er niet aan denken dat kwaadwillenden toegang hebben tot je mail. Het is **echt** niet leuk om te moeten proberen zo'n puinhoop op te ruimen. Dat gaat je dagen/weken kosten.

Tot Slot

En nu, nu we overal tweestapsverificatie gebruiken, kunnen we dan weer overal een en hetzelfde wachtwoord gebruiken. Ik begrijp de gedachte, maar helaas; doe het niet! Als je al een wachtwoord hebt dat alles kan ontsluiten, dan is het alleen het wachtwoord dat je voor je **wachtwoordkluis** gebruikt. Dat is waarschijnlijk het belangrijkste wachtwoord dat je hebt. Dat is bij mij een wachtwoord dat meer dan dertig tekens omvat en ook wordt beveiligd met 2FA! Gebruik jij ook een wachtwoordkluis? Beveilig deze dan met tweestapsverificatie !

O ja, voor je eigen veiligheid is het niet verstandig om een apparaat als 'vertrouwd' te markeren. Natuurlijk is dat gemakkelijk, maar het schakelt voor dat apparaat de tweestapsverificatie uit. Dat is dus niet wijs. Het doel van 2FA is immers het beschermen van jouw persoonlijke en financiële gegevens. Dat wordt door het als 'vertrouwd' markeren tenietgedaan.

Links

1. Authy https://bit.ly/r-hndla
2. DeepL https://bit.ly/r-deepl
3. iDIN https://bit.ly/r-idin
4. Man-in-the-Middle https://bit.ly/r-mim
5. Fido2-sleutel https://bit.ly/r-fido2
6. DigiD https://bit.ly/r-digid
7. WhatsApp https://bit.ly/r-wap
8. Wie ondersteunen 2FA https://bit.ly/r-tfa
9. Mijn andere artikelen https://bit.ly/r-art
10. Dit artikel – groeiend - https://bit.ly/r-mfa