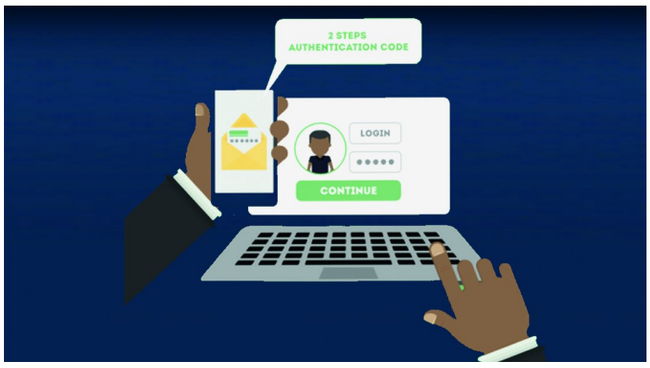
Tweestapsverificatie

Rein de Jong

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 achterhalen. 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.

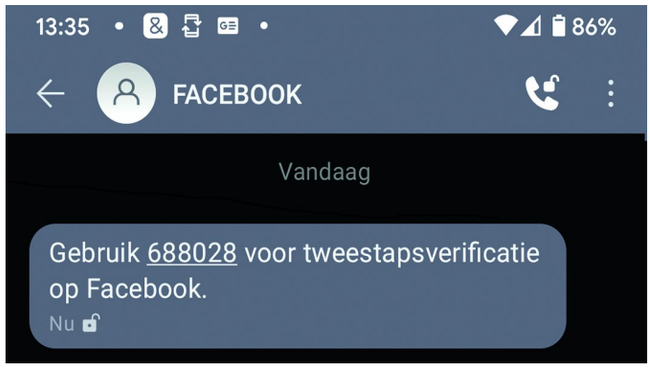
Ik probeer hier uit te leggen wat tweestapsverificatie, ook bekend als Twee Factor Authentication (2FA), precies inhoudt; hoe het werkt en de manier waarop het bijdraagt aan een veiligere manier van verificatie, wat de hindernissen zijn en waarom je het zou moeten gebruiken. Het beschrijft ook aanbieders 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 de 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 verschillende extra componenten bestaan. Eén daarvan is 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 veel veiliger dan statische wachtwoorden.

Nadelen:
- Er is een beperkt aantal pogingen toegestaan waardoor het risico op kraken wordt verkleind
- 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)

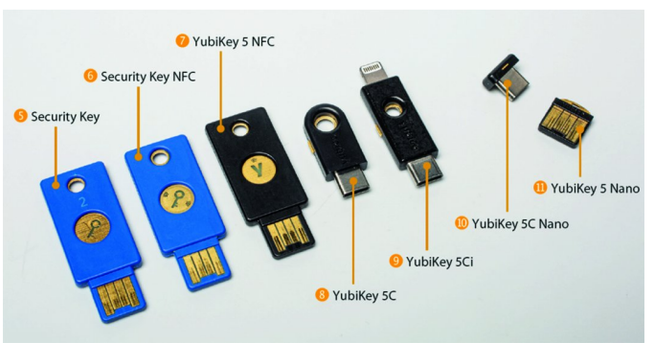
Door je mobiele nummer te delen met de betreffende dienst geef je privacy prijs.
Bovengenoemde nadelen kunnen worden voorkomen door een authenticator-app te gebruiken. Een auhenticator-app genereert codes die je als tweede factor kunt invoeren bij een daarvoor geschikte dienst. Het meest bekend is de 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 er 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; 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 is 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 tweestapsverificatiemiddel dat er is en kan een gebruikersnaam/wachtwoordcombinatie overbodig maken. Lees meer in het online artikel van c't[5]. 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 om te delen
- Het kan erg makkelijk worden meegenomen
- De code verandert periodiek, zodat 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 volgens mij 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

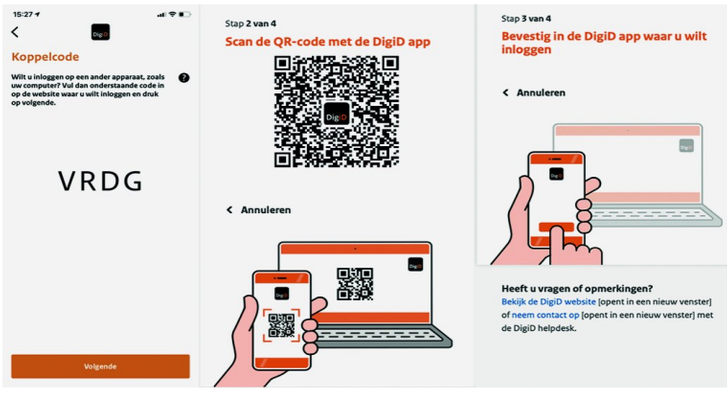
De overheid heeft de DigiD[6] ingesteld om je eenduidig te kunnen identificeren bij instellingen die wettelijk bevoegd zijn om Burgerservicenummers (BSN) te gebruiken, zoals overheidsinstellingen, pensioenfondsen, het onderwijs, de zorg en zorgverzekeraars. Iedere ander bedrijf of organisatie mag dus nooit, maar dan ook nooit, je BSN vragen, laat staan opslaan!

Met de DigiD toon je aan 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, maar 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 zakendoen 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.



En groeiend

De andere diensten beschrijf ik in deel twee van dit artikel, dat in het volgende nummer komt; kun je niet wachten, kijk dan op mijn site[9] en zoek dit artikel. In de loop der tijd worden meer diensten waar je 2FA kunt gebruiken toegevoegd.

Bij het uitkomen van het blad is daar waarschijnlijk al een aantal van onderstaande diensten aan toegevoegd.

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

Zelf uitvinden of een site 2FA ondersteunt

Hoewel hier veel financiële, sociale en opslagdiensten 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 gebruikersgegevens omgaan en dring eropaan dat dit alsnog wordt gecorrigeerd.

Wat moet je nog meer weten over 2FA?

Aangezien je mailaccounts de **'belangrijkste accounts'** zijn die je hebt, is elk mailaccount uiteraard beveiligd met 2FA! Bedenk maar eens 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 (januari 2021) **minimaal vijftien tekens**, maar liever nog langer, om een brute krachtaanval te kunnen weerstaan.
Hackers kunnen je heel veel schade en ongemak berokkenen wanneer zij 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. Wie ondersteunen 2FA	https://bit.ly/r-tfa
8. Mijn andere artikelen	https://bit.ly/r-art
9. Dit artikel - groeiend -	https://bit.ly/r-mfa