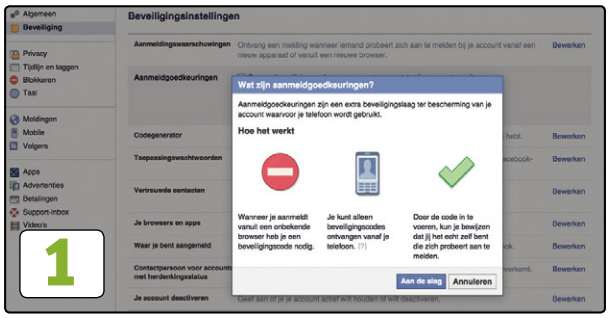
Tweestaps-authenticatie

Een extra stapje

U kunt nog zulke sterke wachtwoorden gebruiken, helemaal veilig bent u nooit. Want wat als er malware op uw pc komt, of als de database van bijvoorbeeld een webwinkel waar u wel eens wat gekocht hebt wordt gehackt? Daarom werken steeds meer online diensten met tweestaps-authenticatie. Hiermee voegt u een extra beveiliging toe aan uw privégegevens.

We weten inmiddels allemaal wel dat het verstandig is om een goed wachtwoord te gebruiken: niet te kort, liever geen woorden die in het woordenboek staan en het liefst een mix van grote letters, kleine letters, cijfers en leestekens. Toch is een lastig te kraken wachtwoord niet altijd voldoende. Via malware kunnen internetcriminelen alsnog uw wachtwoord achterhalen, online diensten kunnen gehackt worden of er kijkt simpelweg iemand over uw schouder mee terwijl u inlogt op Facebook of Gmail. Onder andere Microsoft, Google en Facebook hebben daarom extra beveiliging toegevoegd. Naast het invullen van uw gebruikersnaam en wachtwoord dient u nog een handeling uit te voeren om in te kunnen loggen. Dat kan zijn het invullen van een code die u via sms of een speciale app ontvangt, of door een speciale usb-stick in uw pc of Mac te stoppen. Het is wat extra werk, maar uw gegevens zijn een stuk beter beveiligd.



Facebook gebruikt sms'jes als extra beveiliging voor het inloggen.

Sms van Facebook

Facebook ondersteunt al sinds een aantal jaren het inloggen in twee stappen. Het sociale netwerk werkt hiervoor met een code die per sms wordt verzonden. Het is hiervoor dus wel noodzakelijk dat er een mobiel nummer is gekoppeld aan het Facebook-account. Om de extra beveiliging bij Facebook in te schakelen, klikt u op de desktopversie van de website rechtsboven op het pijltje en kiest u voor Instellingen. Daar gaat u naar Beveiliging en de optie Aanmeldgoedkeuringen. Via Bewerken kunt u deze optie instellen. Facebook stuurt vervolgens al tijdens het proces een sms'je met een code om de extra beveiliging in te schakelen **(afbeelding 1)**.

Speciale Microsoft-app

Zoals gezegd gebruikt ook Microsoft tweestaps-authenticatie, of 'verificatie in twee stappen', zoals Microsoft het noemt. Dit is niet alleen handig om veilig in te kunnen loggen op de website van Microsoft zelf, maar ook bij veel andere sites en diensten. Microsoft heeft zelf een heleboel sites en apps die van dezelfde inloggegevens gebruik maken: denk aan e-mail en het Xbox-netwerk. Ook is het mogelijk om bij sites van andere bedrijven in te loggen door gebruik te maken van uw account bij Microsoft. De extra beveiliging kan dus worden gebruikt om veel sites en diensten veilig te gebruiken.

Microsoft gebruikt voor tweestaps-authenticatie geen sms, maar heeft liever dat u voor het veilig inloggen een speciale app gebruikt. Het inschakelen van verificatie in twee stappen gaat via de Microsoft-website op account.microsoft.com. Daar logt u in met uw gebruikersnaam en wachtwoord, bijvoorbeeld die van Outlook of Live Mail. Op het tabblad Beveiliging en privacy gaat u naar de optie Meer beveiligingsinstellingen. Door een stukje naar beneden te scrollen, komt u bij de optie Verificatie in twee stappen instellen. Microsoft laat u vervolgens kiezen voor welk mobiel platform u de verificatie-app wilt gebruiken. Voor Windows Phone heet die Authenticator en die voor Android draagt de naam Microsoft-account. Voor iOS en andere platformen stuurt Microsoft u door naar de app Google Authenticator, inderdaad van de concurrent. Meer daarover verderop in dit artikel.

Om te controleren of het inlogverzoek correct is, toont Microsoft in het groen een code die overeen moet komen met die op de site waarop u probeert in te loggen.

Inloggen via de Microsoft-app werkt kinderlijk eenvoudig. Wanneer u bijvoorbeeld probeert in te loggen op de website van Microsoft om uw account-gegevens aan te passen, vult u zoals gewoonlijk uw gebruikersnaam en wachtwoord in. Daarna wordt u een scherm voorgeschoteld waarop u een verificatiecode kunt invullen. Microsoft voegt daar nog een eigen code, bestaande uit letters en cijfers, aan toe. Tegelijkertijd krijgt u een melding van de verificatie-app dat er een poging wordt gedaan om in te loggen. Om te controleren of het verzoek om in te loggen correct is, laat de app – als het goed is – dezelfde code zien die bij het inlogscherm wordt getoond **(afbeelding 2)**. Klopt dit, dan kunt u in de app met een druk op 'Goedkeuren' de inlogpoging door laten gaan. Vervolgens wordt u automatisch ingelogd op de Microsoft-site.

Inloggen via Google

Google pakt het ongeveer hetzelfde aan als Microsoft als het gaat om het inloggen in twee stappen. Voor zowel Android als iOS is de app Google Authenticator beschikbaar. Bezitters van een iPhone of iPad worden al door Microsoft doorgestuurd naar deze app om veilig in te loggen, maar ook op Android kunt u met een Microsoft-account de Google-app gebruiken. Wanneer u deze app wilt gebruiken met een Android-account, kiest u bij het instellen van verificatie in twee stappen opnieuw voor de optie Android. In het volgende scherm klikt u dan op Probeer dan deze app, onder aan het scherm **(afbeelding 3)**. Vervolgens krijgt u een link naar de Google-app in de Play Store. Om de Google Authenticator-app te koppelen aan bijvoorbeeld het Microsoft-account dient u via de app de gegeven qr-code te scannen. Dat gaat in de app via het menu rechtsboven en dan de opties Account instellen en Een streepjescode scannen.

Met tweestaps-authenticatie inloggen via de Google-app gaat iets anders in zijn werk dan bij Microsoft. U krijgt geen melding bij een nieuw inlogverzoek. Daarentegen genereert de app telkens nieuwe codes voor de diverse diensten. Als u dus wilt inloggen, vult u de code in die op dat moment in de app wordt getoond **(afbeelding 4)**.

Natuurlijk is het ook mogelijk om bij Google zelf, of bij diensten die zijn gekoppeld aan een Google-account, in te loggen via tweestaps-authenticatie. Het instellen hiervan gaat via accounts.google.com. Daar kunt u via de optie Inloggen bij Google en daarna Authenticatie in twee stappen het veilig inloggen inschakelen.

Microsoft geeft ook bij Android de optie om de Google-app te gebruiken, in plaats van de eigen app.

Een account toevoegen aan de Google Authenticator-app gaat door middel van het scannen van een qr-code.

Nog een stap verder

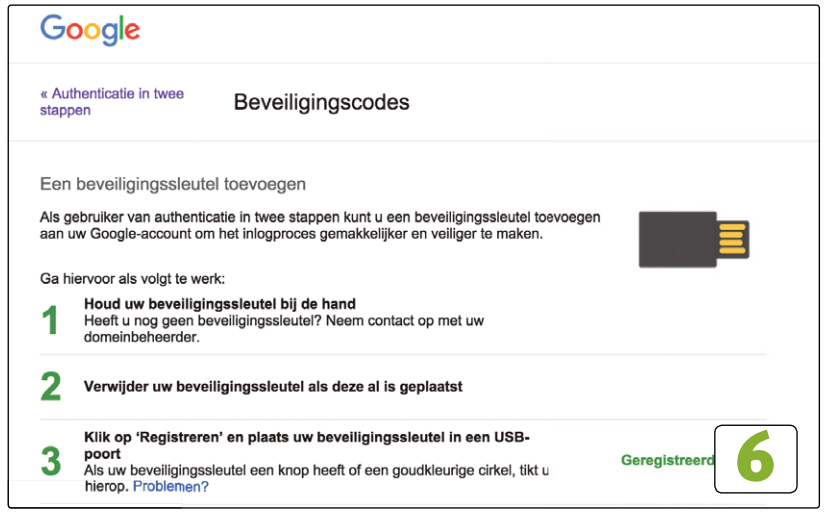
Google biedt de mogelijkheid om niet via codes uit een app, maar met een speciale usb-stick in te loggen. Deze beveiligingssleutels maken gebruik van Universal 2nd Factor, kortweg U2F. Die standaard is ontwikkeld door Google, samen met Yubico. Dit laatste bedrijf verkoopt deze sleutels onder de naam Yubikey. Let bij aanschaf van zo'n sleutel wel op dat u een model hebt dat U2F ondersteunt, zoals de Yubikey Edge of Neo. Deze zijn in Nederland onder andere te verkrijgen via www.yubikeyshop.nl **(afbeelding 5)**.

De U2F-sleutel gaat in de usb-ingang van een laptop, pc of Mac. Hij werkt op alle apparaten die kunnen werken met usb-toetsenborden. De enige beperking voor het gebruik van de U2F-sleutels is dat ze vooralsnog alleen werken in Google Chrome.

Het aanmelden van een beveiligingssleutel bij Google gaat via hetzelfde menu als het instellen van tweestaps-authenticatie. Daar klikt u op het tabblad Beveiligingscodes op Beheren en daarna op Beveiligingssleutel toevoegen. Vervolgens klikt u op Registreren, stopt u de sleutel in uw computer en drukt u op het goudkleurige rondje op de sleutel. Als alles goed gaat, wordt de sleutel herkend en direct geregistreerd **(afbeelding 6)**.

De sleutel gebruiken is eenvoudig. Het enige dat u hoeft te doen is ervoor te zorgen dat de stick in de laptop of pc zit wanneer u bij een Google-dienst wilt inloggen, waarbij het goudkleurige rondje indrukt.

Google is niet de enige die deze manier van veilig inloggen ondersteunt. Wachtwoordenkluis Lastpass ondersteunt al enige tijd U2F en onlangs kwam ook Dropbox met het nieuws dat het met de standaard werkt.



Google biedt de optie om tweestaps-authenticatie te gebruiken via U2F-sticks.

De U2F-sleutel van Yubico.

Tekst: Jeroen van de Nieuwenhof