Inhoud

1. 2 FACTOR AUTHENTICATIE

Wij zien ons door de huidige ontwikkelingen omtrent cybercriminaliteit genoodzaakt om de beveiliging van onze systemen en web applicaties, en daarmee de privacy gevoelige informatie, beter te beschermen. Om dit te bewerkstelligen hebben wij uw medewerking nodig!

Een 2 factor authenticatie is een extra beveiligingslaag die is ontworpen om ervoor te zorgen dat u de enige persoon bent die toegang heeft tot uw account, zelfs als iemand uw wachtwoord weet.

1.1 DE WERKING VAN 2 FACTOR AUTHENTICATIE

Zoals hierboven beschreven zorgt de 2 factor authenticatie ervoor dat alleen u toegang heeft tot uw account. Wanneer u inlogt wordt u gevraagd om uw gebruikersnaam, wachtwoord en een zescijferige verificatiecode.

De zescijferige verificatiecode wordt door een authenticatieapp gegenereerd. Deze code is voor 30 seconden geldig, voordat een nieuwe code wordt gegenereerd. Hierdoor verkleint u de kans aanzienlijk dat kwaadwillenden toegang hebben tot uw account.

Er zijn meerdere authenticatieapps te downloaden voor IOS- en Android-gebruikers. De meest bekende zijn: Google Authenticator en Microsoft Authenticator.

De te downloaden authenticatieapps zijn gratis en volledig Nederlandstalig. Ze zijn overigens ook in andere talen beschikbaar.

Let op: hoewel de 2 factor authenticatie ervoor zorgt dat er een extra beveiligingslaag wordt toegevoegd, is vooral de combinatie van een sterk wachtwoord en de 2 factor authenticatie belangrijk. Zorg er dus voor dat uw wachtwoord minimaal 15 tekens bevat. Verwerk in uw wachtwoord hoofdletters, kleine letters, cijfers en symbolen om het voor kwaadwillenden lastig te maken om uw wachtwoord te achterhalen.

2. GOOGLE AUTHENTICATOR

Zoals genoemd zijn er meerdere authenticatieapps beschikbaar. Om u op weg te helpen leggen wij u in deze handleiding uit hoe u stap-voor-stap de Google Authenticator installeert. U kunt er ook voor kiezen om een andere authenticatieapp te downloaden.

De Google Authenticator is een gratis app die u op uw smartphone of uw tablet kunt installeren en die een zescijferige code genereerd. NB deze app kunt u niet op uw PC installeren.

Na het inloggen op een website of app die een 2 factor authenticatie vereist, kunt u de code van de Google Authenticator invoeren.
In uw geval zal Nmbrs na het inloggen met uw gebruikersnaam en wachtwoord via uw webbrowser de extra code vragen. U vult hier de zescijferige verificatiecode in die de Google Authenticator heeft gegenereerd. Hoe u deze zescijferige verificatiecode ontvangt, leggen wij hieronder aan u uit.

2.1 INSTALLATIE GOOGLE AUTHENTICATOR

Om Google Authenticator te gebruiken, heeft u minimaal Android-versie 4.4 of een iPhone 3G.

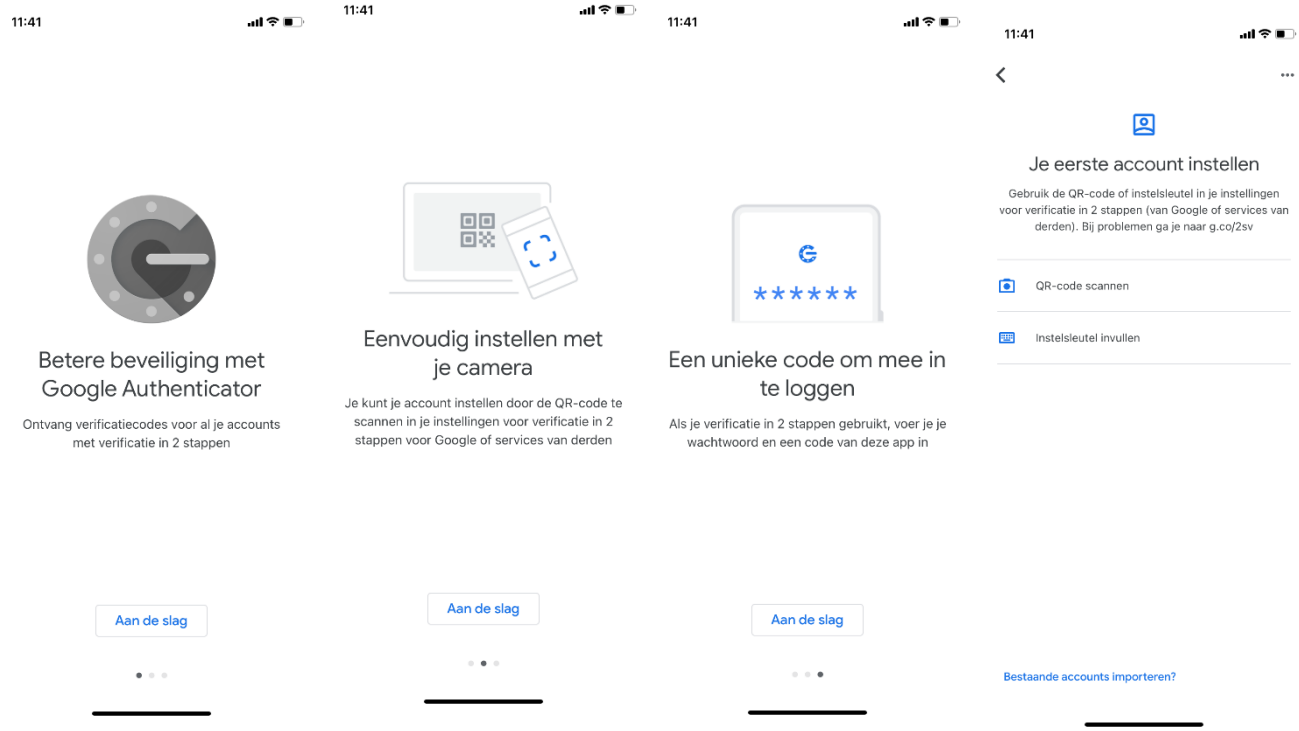
Tip: zorg ervoor dat u voorafgaand aan de download van de app verbonden bent met een Wifi-netwerk, om eventuele kosten voor de internetverbinding te vermijden.

<u>Stap 1</u>
Download de Google Authenticator app op je smartphone of tablet. Deze is beschikbaar voor Android in de Google Play Store en voor IOS gebruikers in de App Store.

Zodra u de Google Authenticator app hebt gedownload, klikt u op het pictogram van de Google Authenticator app op uw smartphone of tablet om de app te starten.

Stap 2

Wanneer u de Google Authenticator app voor de eerste keer gebruikt, klikt u op ‘Aan de slag’. U klikt vervolgens op ‘QR-code scannen’. Zie afbeeldingen hieronder:



Indien u nog geen app op uw tablet of telefoon heeft waarmee u een QR-code kunt scannen, dan kan nu gevraagd worden of u nu zo’n app wilt downloaden en installeren.

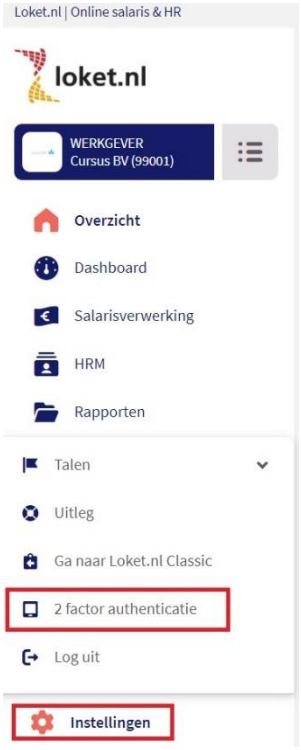
Er zijn meerdere QR-code scanners in de PlayStore of Apple Store verkrijgbaar en allemaal met hetzelfde doel. Het maakt dus niet uit welke u download.

Uw tablet of smartphone kan u vragen om Google Authenticator toegang te geven (autoriseren) tot uw camera, voor het scannen van een QR-code.

3 2 Factor authenticatie in Loket.nl

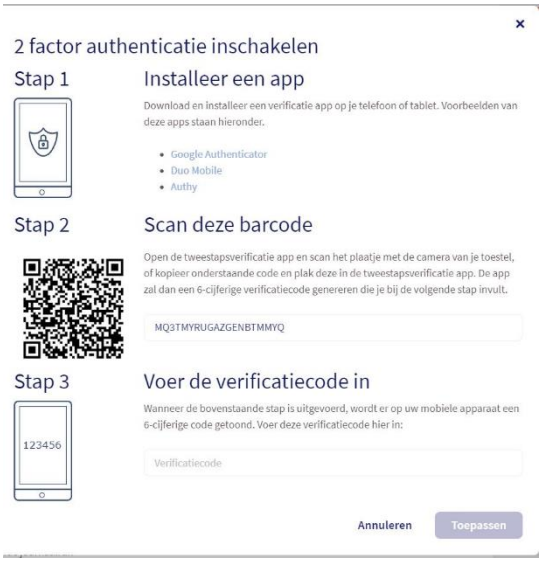
3.1 2 factor authenticatie voor werkgevers

3.1.1 Activeren in Loket.nl



Alle gebruikers van Loket.nl hebben de mogelijkheid om de extra beveiliging voor het inloggen te activeren. Linksonder via de button ‘instellingen’ verschijnt de nieuwe menuoptie ‘2 factor authenticatie’.
Zie linker afbeelding.

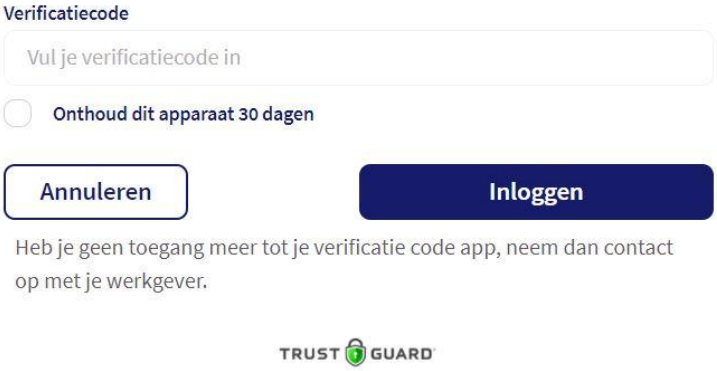
Kies je voor deze menu-optie? Dan verschijnt het volgende scherm, zie afbeelding rechts:



Doorloop eenmalig de procedure en 2 factor authenticatie is voor jou geactiveerd. Je krijgt hiervan een melding rechtsboven in je scherm.

3.1.2 Inloggen Loket.nl

Zodra je inlogt en je gebruikersnaam en wachtwoord hebt opgegeven, verschijnt dit scherm, zie rechts:



Vul hier de code in die je terug kunt vinden in de app die op je mobile device is geïnstalleerd. De code die in de app wordt gegenereerd, is een beperkte tijd geldig.

3.1.3 Onthoud dit apparaat 30 dagen

Vink je de mogelijkheid ‘Onthoud dit apparaat 30 dagen’ aan, dan zal de browser van het apparaat waarop je inlogt de inlog 30 dagen onthouden, zodat je niet telkens de verificatiecode hoeft in te vullen. Let op: deze functie werkt alleen op het apparaat waar je op dat moment op werkt.

3.1.4 Deactiveren 2 factor authenticator in Loket.nl

Wil je geen gebruik meer maken van de 2 factor authenticatie mogelijkheid? Klik linksonde op de button ‘instellingen’ en klik op ‘2 factor authenticatie. Onderstaan scherm verschijnt. Vul de door de app gegenereerde code in en klik op de opslaan button.

Gezien de ontwikkelingen geschreven in de inleiding van dit document, raden wij af om een 2 factor authenticatie uit te schakelen.

3.2 Kun je niet meer inloggen?

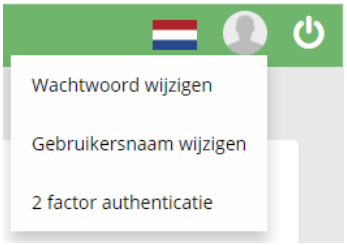
Neem dan contact met ons op via hrs@crowefoederer.nl.

3.2 2 factor authenticatie voor werknemers (Werknemerloket)

In het Werknemerloket is het mogelijk om voor het extra beveiligen van je toegang in te loggen via 2 factor authenticatie. Naast het invullen van je gebruikersnaam en wachtwoord heb je in dat geval je mobiele telefoon of tablet nodig om de extra beveiligingsstap bij het inloggen te kunnen uitvoeren.

3.2.1 Activeren in het Werknemersloket

Alle gebruikers van het Werknemersloket krijgen de mogelijkheid om de extra beveiliging voor het inloggen te activeren. Rechtsboven onder het icoontje van een persoon (silhouet) verschijnt de nieuwe menuoptie ‘Two factor authenticatie’.

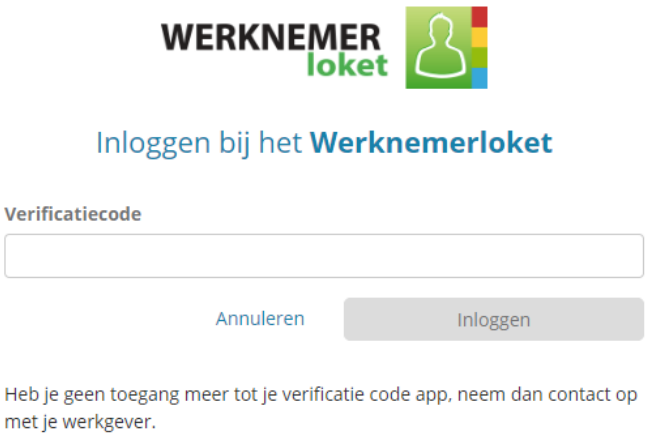


Kies je voor deze menuoptie, dan verschijnt het volgende stappenplan:

Doorloop eenmalig deze procedure en 2 factor authenticatie is voor jou geactiveerd.

3.2.2 Inloggen Werknemerloket

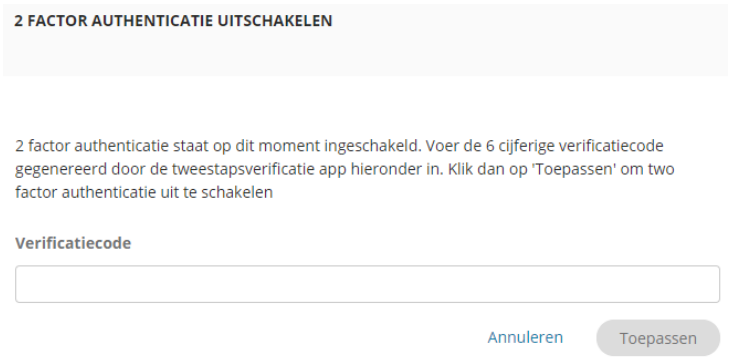
Zodra je inlogt en je gebruikersnaam en wachtwoord hebt opgegeven, verschijnt onderstaand scherm:



Vul hier de code in die je in de Google authenticator terug kunt vinden. Let op: de code die in de app wordt gegenereerd, is voor beperkte tijd geldig.

3.2.3 Deactiveren in het Werknemerloket

Wil je geen gebruik meer maken van de 2 factor authenticatie mogelijkheid? Klik rechtsboven op het silhouet en klik vervolgens op '2 factor authenticatie'. Het volgende scherm verschijnt.



Vul de door Google authenticator gegenereerde code in en klik op 'toepassen'.

3.2.4 Kun je niet meer inloggen?

Kun je om wat voor reden dan ook niet meer inloggen met je verificatiecode? Neem dan contact op met je werkgever, deze kan de verificatie voor je uitzetten, zodat je bovenstaande acties weer opnieuw kunt instellen.

De werkgever kan in Loket.nl waar hij ook toegang verstrekt tot het Werknemerloket het veld 'Tweestapsverificatie' op 'Nee' zetten. Let op: dit kan alleen wanneer er direct in Loket wordt ingelogd, middels een SSO-koppeling gaat dit niet.

Je kunt als werknemer nu inloggen met alleen gebruikersnaam en wachtwoord. In het Werknemerloket is het mogelijk om de 2 factor authenticatie weer te activeren.

F.A.Q.

Wat betekent 2 factor authentication?
2 factor authentication verwijst naar een beveiligingsmethode die wordt gebruikt om accounts en systemen te beschermen tegen ongeautoriseerde toegang. Gebruikers worden verplicht om zichzelf te verifiëren met een door de authentication app gegenereerde code.

2 factor authentication kan worden gebruikt om de beveiliging van een telefoon, een online account of zelfs een deur te versterken. Het werkt door twee soorten informatie van de gebruiker te eisen: De eerste is een wachtwoord of PIN, en de tweede een vingerafdruk of eenmalige code die naar je telefoon wordt verzonden.

Wat is een 2 factor authenticator?
Met de 2 factor authenticator wordt er een eenmalige code gegenereerd om de identiteit van een gebruiker te bewijzen wanneer deze probeert toegang te krijgen tot een online account of systeem. De code wordt via sms verzonden naar een telefoonnummer of per e-mail dat gekoppeld is aan de gebruiker. Je krijgt pas toegang tot een account wanneer de 2 factor authentication juist is ingevoerd.

Kan een 2 factor authenticator gehackt worden?
Hoewel het mogelijk is om 2 factor authenticator te hacken, is de kans erg klein en is 2 factor authentication zeker de beste manier om accounts en systemen veilig te houden.

Een manier waarop 2 factor authentication gehackt kan worden, is via de SMS-methode. Dit is een methode waar een eenmalige code wordt verzonden naar het telefoonnummer van een gebruiker.

Er zijn verhalen bekend over hackers die de mobiele telefoonaanbieders misleiden om het telefoonnummer van iemand anders over te zetten naar hun eigen telefoon. De hackers nemen contact op met de providers die zich voordoen als klant en vragen om een nieuwe simkaart met het nummer van het slachtoffer. Ze hebben dan toegang tot elke authenticatiecode die aan dat telefoonnummer is verbonden.

Dit komt echter zelden voor. Het zeer kleine risico van gehackt kunnen worden, weegt niet op tegen de voordelen van 2 factor authentication. Dit is en blijft een heel sterk hulpmiddel in de strijd tegen cyberaanvallen en identiteitsfraude.

Ik wissel binnenkort van toestel. Hoe zet ik de Google Authenticator over?
Als u wisselt van smartphone, zet dan eerst de koppeling via de app uit voordat u hem verwijdert. De authenticatieapp is gebonden met uw toestel. Installeer op uw nieuwe smartphone opnieuw de Google Authenticator app en koppel uw account.

Ik heb een probleem met de Google Authenticator App en deze staat hier niet genoemd. Waar kan ik een antwoord op mijn vraag vinden?
Indien er een probleem is met de Google Authenticator App die hierboven niet is behandeld, dan raden wij u aan om op de supportsite van Google te kijken. Zij hebben wellicht uw vraag behandeld in één van de vele artikelen: support.google.com.