

Wachtwoord managers

Rik Deschamps - december 2022



Wat is het probleem?

Wachtwoorden zijn een sleutel element in cybersecurity.

Ze zorgen ervoor dat onze gegevens beveiligd en onze privacy gewaarborgd blijft.

We botsen echter meer en meer op de limieten van een goed wachtwoordbeheer, vooral binnen ons doelpubliek de senioren.

Immers, de steeds dwingender eisen van een goed beheer (aantal, kenmerken... van wachtwoorden) conflicteert met de beperkte geheugen- en andere mogelijkheden van onze gebruikers.

Het gebruik van een goeie en gebruiksvriendelijke **tool** ivm wachtwoordbeheer is daarom onontbeerlijk geworden.

Eisen ivm wachtwoorden.

1. Moeten geheim zijn en blijven.
 - a. Regelmatig hernieuwen
 - b. Onderling verschillend
 - c. Nooit doorgeven aan derden
 - d. Niet opschrijven
 - e. Niet op publieke computers gebruiken
 - f. Niet opslaan op PC - laptop - smartphone
2. Moeten moeilijk zijn.
 - a. Voldoende lang - min 9 karakters
 - b. Voldoende complex (letters -groot en klein-, cijfers en speciale tekens
 - c. Geen 'evidente' elementen (namen - datums...) bevatten.

Wat is een wachtwoord manager?

Een wachtwoordmanager is een **digitale 'kluis'** waarin je al je wachtwoorden en gebruikersnamen kunt opslaan. Je hoeft dan alleen het wachtwoord van je wachtwoordmanager te onthouden. En bezoek je een website, dan vult de wachtwoordmanager automatisch je gebruikersnaam en wachtwoord in. Ook wanneer je een app op smartphone of iPhone opent zal dit gebeuren indien relevant.

Het is wel belangrijk een **sterk wachtwoord** voor je wachtwoordmanager te kiezen.

Soorten wachtwoordmanagers.

1. Online managers versus offline managers.
 - a. Offline managers plaatsen info enkel op het toestel - deze categorie verdwijnt stilaan.
 - b. Online managers halen info op vanuit de cloud en kunnen tussen toestellen en besturingssystemen gebruikt worden.
2. Onafhankelijk versus geïntegreerd.
 - a. Onafhankelijke (standalone) producten
 - b. Geïntegreerd in besturingssysteem of browser
3. Gratis versus betalend.

=> dikwijls gedeeltelijk betalend (freemium)
4. Thirdparty versus opensource

<u>Naam</u>	<u>Browser Besturing</u>	<u>Prijs</u>	<u>generatie wachtw.</u>	<u>im/export</u>	<u>beveiliging</u>	<u>2-staps verificatie</u>	<u>opslag?</u>
Lockwise	Mozilla	gratis	beperkt	ja	master wachtw.	authenticatie app	lokaal in browser
Edge	Edge Windows	gratis	nihil	ja	uitgebreid	ja & auth.app	lokaal of server MS
Brave	Brave	gratis	nihil	beperkt	ok	nihil	onduidelijk
Chrome	Chrome Android	gratis	ok	uitgebreid	uitgebreid	ja & auth.app	google cloud-acct
Lastpass	onafhankelijk browser+telef	freemium	ja	ja	beperkt	ja	server vault
Dashlane	onafhankelijk pc + telefoons	freemium (1 toestel)	in add-on betalend	csv-format	uitgebreid	ja	cloud waar?
Bitwarden	onafhankelijk pc + telefoons	freemium	generator	csv-format	ok maar instell/toes	uitgebreid	cloud in US
1Password	onafhankelijk pc + telefoons	betalend	generator	eigen formaat	ok	ja (betalend)	cloud in EU/US/Cn
Keepass	onafhankelijk enkl windows	gratis ⇒ tweakers	uitgebreid	csv-format	ok	ja maar moeilijk	eigen pc

Google Chrome wachtwoord manager.

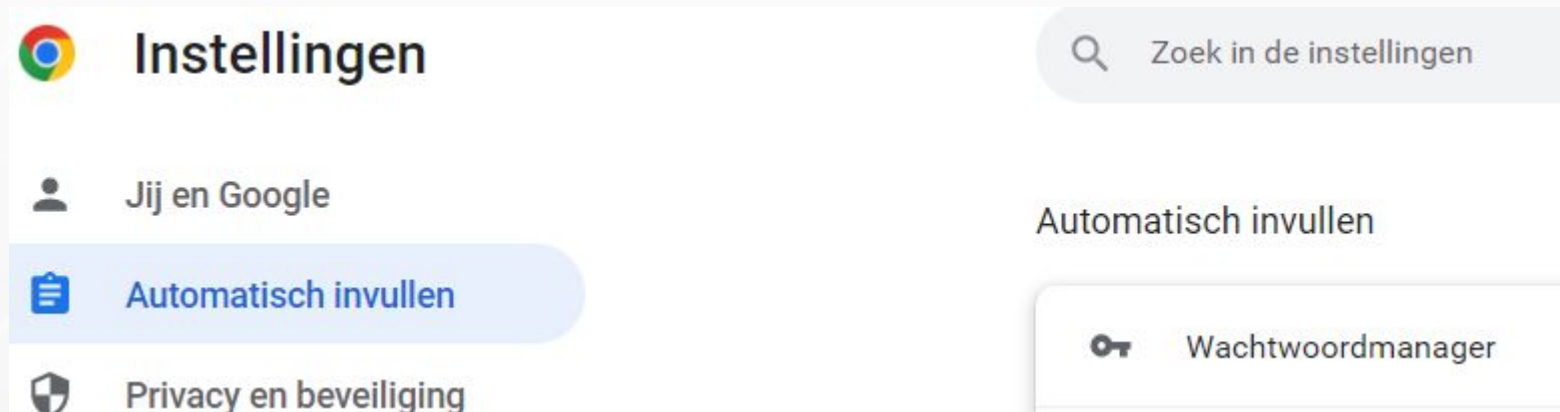
Je kan de opgeslagen wachtwoorden bij gebruik van de Chrome browser (PC en android-toestellen) gebruiken als een kluis.

Het wachtwoord van je Google Account is dan het **master wachtwoord** van je kluis.

Bij iedere aanmaak van een wachtwoord kan de WW-manager een sterk wachtwoord genereren; dit wordt vervolgens opgeslagen in de kluis die op haar beurt gesynchroniseerd wordt op ieder toestel met hetzelfde Google Accct. Bij het inloggen op een website via Chrome (PC of smartphone) of een android-app zal het betreffende WW automatisch uit de kluis opgehaald en gebruikt worden.

Opvragen WW-manager Chrome.

In Chrome via Instellingen / autom invullen / WW-manager



Maak, bewaar en beheer je wachtwoorden zodat je makkelijk kunt inloggen bij sites en apps.

Aanbieden wachtwoorden op te slaan



Automatisch inloggen

Log automatisch in bij sites en apps met je opgeslagen inloggegevens. Als dit uitstaat, moet je elke keer je inloggegevens bevestigen voordat je inlogt op een website.



Wachtwoorden controleren

Bescherm je wachtwoorden tegen gegevenslekken en andere beveiligingsproblemen



Versleuteling op het apparaat

Je wachtwoorden worden versleuteld op je apparaat voordat ze worden opgeslagen in Google Wachtwoordmanager



Opgeslagen wachtwoorden

Toevoegen



← Wachtwoorden controleren



Gecheckte wachtwoorden • Zojust
39 zwakke wachtwoorden

[Nogmaals controleren](#)

Chrome laat het je weten als je inlogt met een gehackt wachtwoord

Zwakke wachtwoorden

Zwakke wachtwoorden zijn makkelijk te raden. Laat Chrome [sterke wachtwoorden voor je instellen en onthouden](#).



bnpparibasfortisasv.benefitsatwork.be
beatrice.verschuere@gm... ..

[Wachtwoord wijzigen](#)



Opgeslagen wachtwoorden

Site

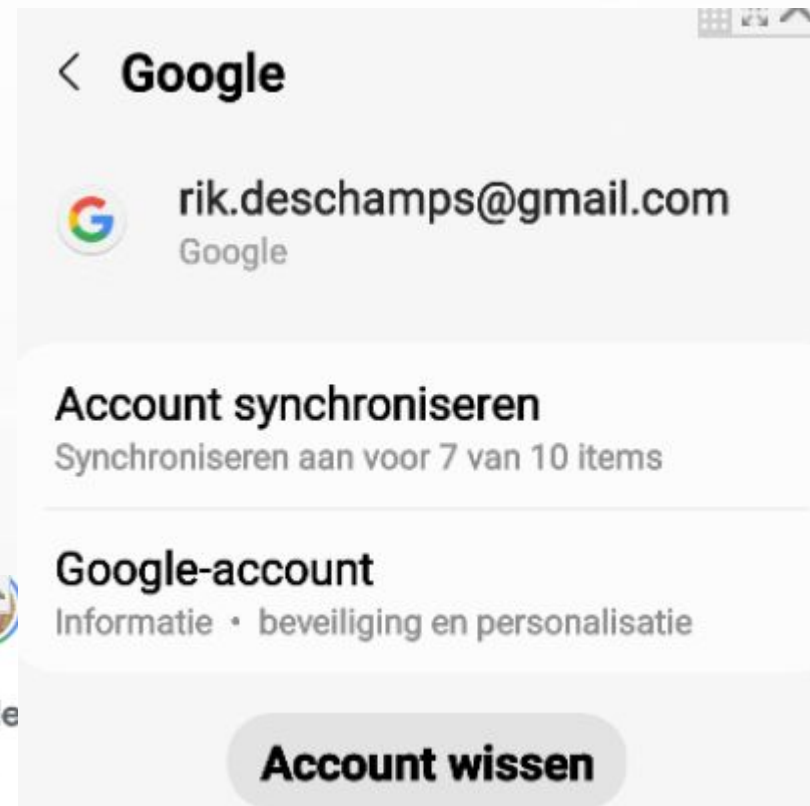
Gebruikersnaam

Wac

Wachtwoorden importeren

Wachtwoorden exporteren

Android



Android/2

Wachtwoordmanager



Maak, bewaar en beheer je wachtwoorden zodat je makkelijk kunt inloggen bij sites en apps. [Meer informatie](#)

Wachtwoordcheck



Check je opgeslagen wachtwoorden om de beveiliging te verbeteren

Wachtwoorden controleren

🔍 92 wachtwoorden doorzoeken +

② 2dehands.be

A acronis.com

🌐 aginsurance.be

Instellingen

Aanbieden wachtwoorden op te slaan



Aanbieden wachtwoorden op te slaan in Android en Chrome

Automatisch inloggen



Automatisch inloggen bij websites met de opgeslagen gegevens. Als de functie uitstaat, wordt elke keer om bevestiging gevraagd voordat je inlogt bij een website.

Wachtwoorden exporteren

Een kopie van je wachtwoorden maken om deze met een andere service te gebruiken



Voeg een snelkoppeling toe aan je startscherm



Voeg Google Wachtwoordmanager toe aan je startscherm om de service sneller te openen

Android/3



Wachtwoordcheck



Wachtwoorden gecheckt voor 92 sites of apps



1 gehackt wachtwoord

Je moet het nu wijzigen



45 hergebruikte wachtwoorden

Maak unieke wachtwoorden



37 zwakke wachtwoorden

Maak sterke wachtwoorden



Nog enkele opmerkingen omtrent Google wachtwoordmanager.

Voordelen:

1. Makkelijk in gebruik voor heel veel mensen met enerzijds een windows-pc en anderzijds een android smartphone
2. Veilig, functioneel rijk, volledig.
 - a. Controle op gehackte WW
 - b. Controle op zwakke WW
 - c. Generator voor sterke WW
 - d. Encryptie op toestel vooraleer te synchroniseren.
 - e. Gratis
 - f. Bruikbaar op alle toestellen

Nadelen:

1. Vendor lock-in: het vereist het blijvend gebruik van Chrome op zowel PC als smartphone/iPhone.