

VEILIG OMGAAN MET WACHTWOORDEN

Zowel in je privé- als beroepsleven heb je voor de computersystemen en websites die je gebruikt vaak een wachtwoord nodig. Al die verschillende wachtwoorden zijn moeilijk te onthouden. Het bijhouden van al die wachtwoorden creëert nieuwe veiligheidsrisico's. Ze bewaren op een blad of in een document is geen goed idee. Dit artikel maakt je wegwijs in hoe je sterke en veilige wachtwoorden kunt aanmaken, hoe je kunt controleren of je wachtwoord veilig en sterk is, wat een *password manager* is en hoe je die kunt gebruiken. Met een voorbeeld in zijn offline- en onlinevariant tonen we hoe je die ook kunt inschakelen in je eigen situatie.

1. GEBRUIK STERKE EN VEILIGE WACHTWOORDEN

Velen onder ons gebruiken voor de hand liggende wachtwoorden die je makkelijk kunt onthouden. Je wilt het jezelf immers niet moeilijk maken en snel kunnen inloggen. En je wilt niet vaststellen dat je je wachtwoord weer vergeten bent en je voor de zoveelste keer op de befaamde knop 'wachtwoord vergeten' moet klikken. Een dergelijke aanpak resulteert vaak in slechte wachtwoorden, zoals bijvoorbeeld '123456', 'paswoord', 'azerty' of de combinatie van je naam en geboortjaar. Ze zijn niet veilig omdat programma's ze makkelijk kunnen kraken.

De website [Saeonweb.be](https://saeonweb.be), een initiatief van de Belgische overheid, geeft een reeks handige tips voor de aanmaak van sterke en veilige wachtwoorden.¹

Wat je zeker WEL moet doen:

- Combineer hoofdletters, kleine letters, cijfers, symbolen en leestekens

Het gebruik van cijfers, hoofdletters, symbolen en leestekens bemoeilijkt het kraken van je wachtwoord omdat het het aantal mogelijk combinaties sterk verhoogt. Je kunt cijfers, hoofdletters en symbolen overal in je wachtwoord of -zin gebruiken.

- Gebruik een lang wachtwoord

Gebruik een wachtwoord dat bestaat uit minstens dertien karakters. Vaak is het gemakkelijker om een wachzin of *passphrase* te onthouden dan een wachtwoord. Je dient dan wel een zin te kiezen die alleen voor jou betekenis heeft, en die niet alleen bestaande woorden bevat. Een voor de hand liggende zin als bijvoorbeeld 'iloveyou' is dus geen goede keuze.

Wat je zeker NIET moet doen:

- Gebruik geen voorspelbaar wachtwoord
- Gebruik geen persoonlijke gegevens, zoals je naam en geboortjaar (bijvoorbeeld 'Jouw-Naam1985').
- Gebruik geen bekende uitdrukkingen, zoals 'Pluk de dag'.
- Gebruik geen teller, zoals 'Plukdedag1', 'Plukdedag2', 'Plukdedag3'...
- Herhaal geen karakters, zoals bijvoorbeeld 'aaabbbccc'.
- Gebruik niet voor elke account hetzelfde wachtwoord

Hetzelfde wachtwoord voor verschillende accounts gebruiken is onverstandig. Als cybercriminelen je wachtwoord voor één website hebben gekraakt, kunnen ze proberen dat wachtwoord ook op andere websites te gebruiken. Het is daarom aangeraden om voor verschillende toepassingen lange en totaal verschillende wachtwoorden te gebruiken, zeker als het gaat om accounts waar je betalingsgegevens of persoonlijke gegevens ingeeft.

- Deel geen wachtwoorden

Het delen van wachtwoorden is onverstandig. Je weet immers nooit wat er gebeurt met je wachtwoord. Als

je toch wachtwoorden wil delen, gebruik dan een *password manager* of wachtwoordkluis (zie verder) om dat op een veilige manier te doen.

- Bewaar wachtwoorden niet zichtbaar

Bewaar je wachtwoorden niet op een opzichtige manier in de buurt van je computer, dus niet gekleefd op je scherm of je bureau. Wachtwoorden bewaar je best ook niet in een e-mail of in een document op je computer, smartphone of tablet.

- Gebruik hetzelfde wachtwoord niet jaren na elkaar

Het is aangeraden om je wachtwoorden regelmatig te wijzigen: jaarlijks voor je privé-accounts, en nog vaker voor je professionele accounts. Wanneer één van je accounts gehackt is, moet je onmiddellijk je wachtwoorden veranderen. Wanneer je je wachtwoord wijzigt, controleer dan steeds eerst of het probleem bij de website is opgelost. Als dat niet het geval is, verander je immers je wachtwoord tevergeefs.

- Gebruik geen 'geheime vragen'

Soms wordt een antwoord op een vraag (bijvoorbeeld 'hoe heet je huisdier?') als wachtwoord gebruikt. Probeer dergelijke geheime vragen te vermijden. Het antwoord erop is immers vaak op het internet terug te vinden.

2. CONTROLEER OF JE PASWOORD VEILIG EN STERK IS

Wil je weten of je al over een goed wachtwoord beschikt? Op de website [How Secure Is My Password](#) kun je testen hoe snel hackers je wachtwoord kunnen kraken. Hoe langer het duurt voor hackers om je wachtwoord te kraken, hoe beter. Om de test te doen vul je op de website je wachtwoord in.



Wij hebben 'azerty' als wachtwoord ingevuld. De website laat weten dat dat wachtwoord onmiddellijk gevonden kan worden omdat het bij de 590 meest gebruikte wachtwoorden hoort. Met de rode kleur duidt de tool aan dat het geen goed wachtwoord is.



Wanneer we 'nastasia' invullen, laat de website weten dat het in vijf seconden gevonden kan worden, omdat het een woord is. Hij vermeldt bovendien dat andere tekens dan letters het wachtwoord moeilijker kunnen maken. 'nastasia1' als wachtwoord ingeven brengt niet veel zoden aan de dijk. Ook dat wachtwoord is te kort en kan op een minuut gevonden worden.



Ook het wachtwoord 'nastasia1!' zal relatief snel gevonden worden, al zal dat nu al wel zestien uren kunnen duren.



We kiezen voor een langer wachtwoord, en gaan voor een wachtzin. Dat is een volledige zin in plaats van een korte opeenvolging van letters, cijfers en tekens bij een wachtwoord. Een voordeel van een wachtzin is de lengte. Meestal is een wachtzin ook makkelijker te onthouden. We opteren voor 'KoffielsLekker'. De tool geeft aan dat het een computer 837.000 jaar zou kosten om dat wachtwoord te raden.



Als we vervolgens nog cijfers en tekens toevoegen en er 'K0ff1e1sLekker!' van maken, zou het zelfs zestien miljard jaar duren vooraleer een computer het wachtwoord raadt. Tekens en cijfers zijn echter niet noodzakelijk. 'Debrunchwaslekker' vraagt 118 miljard jaar van een computer om de wachtzin te vinden.



Op de website <https://haveibeenpwned.com/> kun je controleren of je al eens slachtoffer geweest ben van een datalek. Indien dat het geval is, verander je best je wachtwoord.

3. GEBRUIK VERIFICATIE IN TWEE STAPPEN

Een aanvullende manier om veiliger met wachtwoorden om te gaan is het gebruik van verificatie in twee stappen. Daarbij wordt meestal gebruik gemaakt van iets dat je weet (bijvoorbeeld een wachtwoord) en iets dat je hebt (bijvoorbeeld een gsm) of iets dat je 'bent' (bijvoorbeeld een vingerafdruk). Het gebruik van verificatie in twee stappen is eenvoudig.



In de eerste stap log je met je wachtwoord in bij je account (bijvoorbeeld Facebook, Twitter, Google of Microsoft). In de tweede stap stuurt die account een code naar je gsm die je invult om toegang te krijgen tot je account. Er zijn ook andere manieren voor verificatie in twee stappen zoals bijvoorbeeld via Google Authenticator App of fysieke keys.

4. GEBRUIK EEN PASSWORD MANAGER OF WACHTWOORDKLUIS

Als je veel complexe wachtwoorden hebt die je moet onthouden, is het een goed idee om een *password manager* of wachtwoordkluis te gebruiken. *Password managers* of wachtwoordmanagers zijn gemaakt om op een veilige manier je accounts en hun bijbehorende wachtwoorden veilig op te slaan in de vorm van een versleutelde databank. De wachtwoordkluis zelf beveilig je met een sterk wachtwoord. Het voordeel daarvan is dat je snel en relatief veilig aan je wachtwoorden kan en dat je in principe maar één wachtwoord moet onthouden. Dat is meteen een belangrijk aandachtspunt. Je versleutelt immers al je wachtwoorden met één wachtwoord. Zorg dus dat je hoofdwachtwoord voldoende lang is en uit hoofdletters, kleine letters, cijfers en leestekens bestaat.

Er zijn verschillende soorten wachtwoordmanagers, die elk hun eigen voor- en nadelen hebben:

- hardwarematige wachtwoordmanager;
- softwarematige wachtwoordmanagers;
- online wachtwoordmanagers.

Hardwarematige wachtwoordmanagers hebben de vorm van een USB-stick, die als fysieke sleutel dient. Het nadeel is dat je die sleutel kan verliezen en dat hij gestolen kan worden. Het voordeel is dat je wachtwoorden offline bijgehouden worden, en ze in principe gevrijwaard blijven van beveiligingsrisico's die kunnen ontstaan door verbinding met het internet of door andere software.

Softwarematige wachtwoordmanagers worden als een programma geïnstalleerd op je computer. Een programma dat loopt op je computer is mogelijk kwetsbaar doordat andere software je computer kan doen vastlopen, of je databank corrupt of onbeschikbaar kan maken. Een voorbeeld van opensourcewachtwoordmanager is KeePass. Dat die wachtwoordmanager opensource is, impliceert dat zijn broncode kan worden ingekeken. Dat is geen overbodige luxe bij software die al je wachtwoorden beheert. Het laat ontwikkelaars ook toe om de broncode te gebruiken opdat de wachtwoordmanager op diverse besturingssystemen en webbrowsers kan draaien (bijvoorbeeld Linux, Windows, MacOS, Firefox en Chrome).²

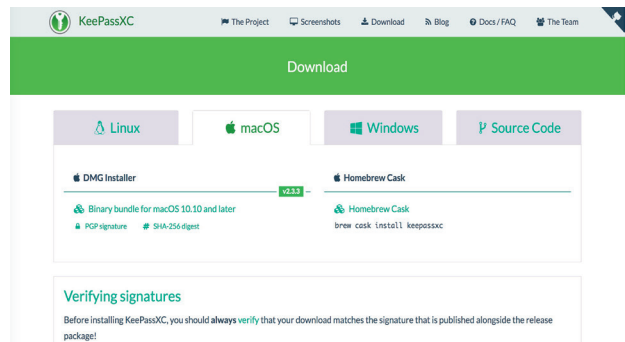
Online wachtwoordmanagers kun je enkel via je webbrowser bereiken. Ze hebben als voordeel dat je wachtwoorden overal bereikbaar zijn. Het nadeel is wel dat je de controle uit handen geeft, en geen zekerheid hebt over wat er met je data (opgeslagen in je wachtwoordendatabank) gebeurt. LastPass en Dashlane zijn voorbeelden van online wachtwoordmanagers. Ze werken als een *cloud service* waarbij je inlogt met je hoofdwachtwoord en je wachtwoorden vervolgens via het internet worden doorgestuurd naar je computer, smartphone of tablet. Meestal wordt LastPass gebruikt als een extensie/add-on van je webbrowser, of als mobiele app. Dashlane biedt ook een lokale installatie aan.³ Het verschil met softwarematige wachtwoordmanagers is dat alle functies gratis kunnen gebruikt worden.

Dit artikel behandelt verder KeePassXC, de desktop-variant van KeePass, en Tusk, de browservariant van KeePass.

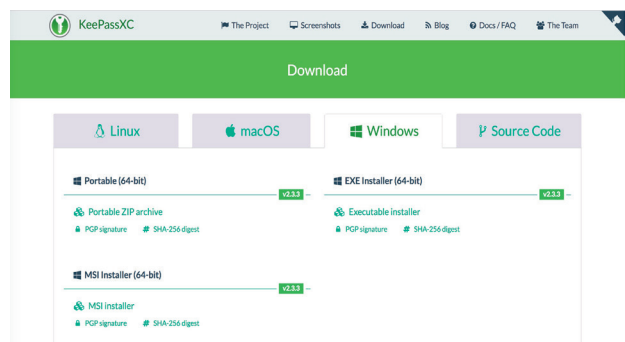
5. BEKNOPTE HANDLEIDING VOOR HET GEBRUIK VAN KEEPASSXC, DE DESKOPTVARIANT VAN KEEPASS

5.1. Download en installeer het KeePassXC

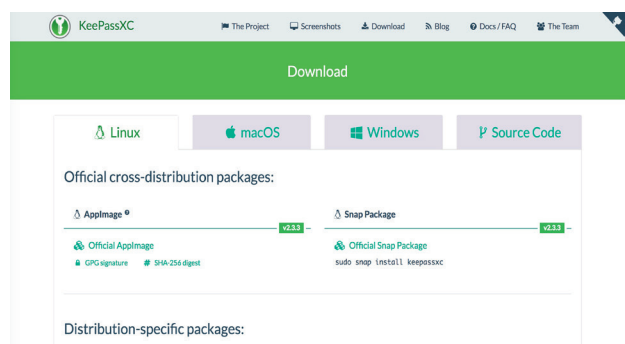
KeePassXC kun je gratis downloaden op <https://keepassxc.org/download/>. Als je KeePassXC downloadt, kun je dat doen voor verschillende besturingssystemen, onder andere voor macOS, Windows en Linux.



Gebruik je macOS, dan kies je hier best de 'DMG installer'.



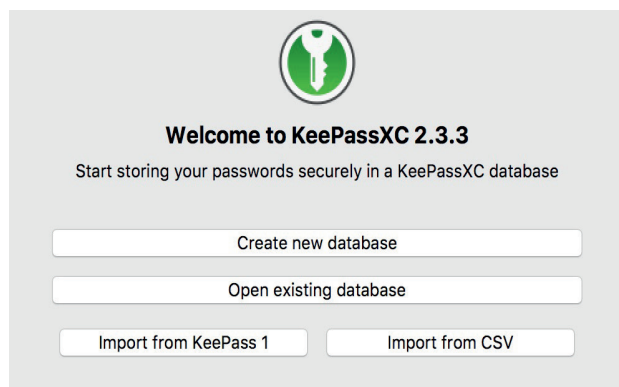
Wil je KeePassXC gebruiken op een recente Windowscomputer, kies dan voor de MSI of de EXE installer 64-bit. Voor oudere Windowssystemen download je beter de 32-bit versie. De *portable* versie van KeePassXC kan geopend worden zonder eerst geïnstalleerd te zijn; dat is interessant als je een computer gebruikt die niet van jou is en waarop je mogelijk geen administratorrechten hebt.



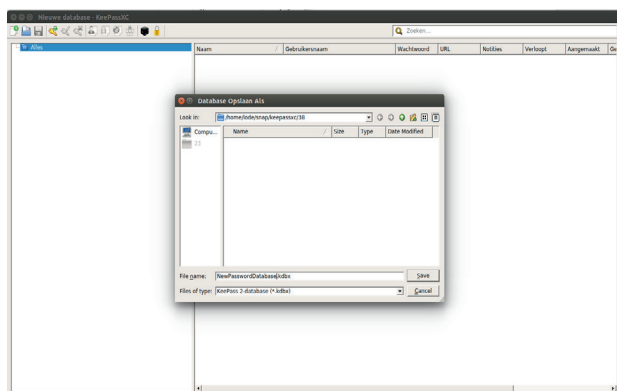
Als je Linux gebruikt, kun je de ApplImage downloaden als je een portable versie wil van KeePassXC. Naast Linux, Ubuntu en Debian ondersteunt KeePassXC ook Fedora, OpenSUSE, Gentoo, Arch-Linux en CentOS. Download het pakket van de website of gebruik het commando dat eronderstaat om KeePassXC via de package manager op je systeem te downloaden en in te installeren.

5.2. Aanmaak van wachtwoordendatabank en hoofdsleutel

Vooraleer je KeePassXC kunt gebruiken, dien je eerst een nieuwe wachtwoordendatabank te maken en een hoofdsleutel in te stellen. Die handelingen zijn op alle platformen ongeveer hetzelfde. Voor dit artikel gebruiken we KeePassXC geïnstalleerd op Ubuntu.

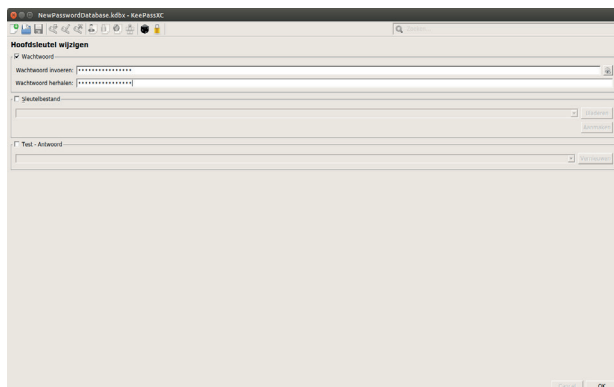


- Open KeePassXC en kies de optie 'Nieuwe databank aanmaken'.
- De software zal je verzoeken om een locatie te selecteren om de nieuwe lege databank op te slaan.

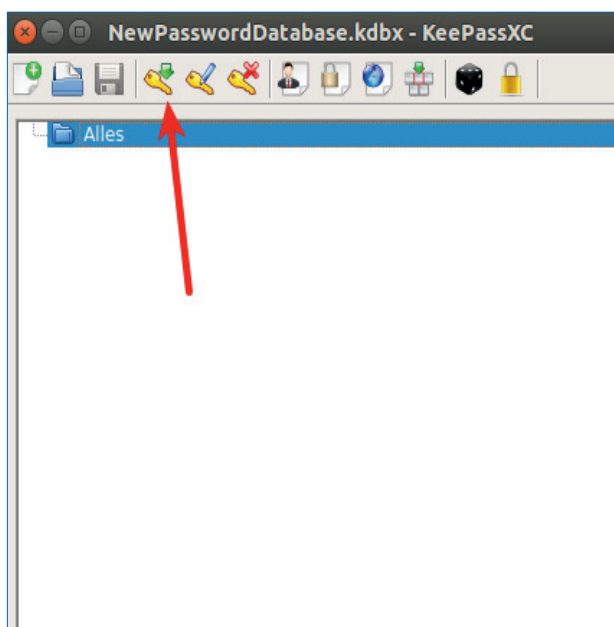


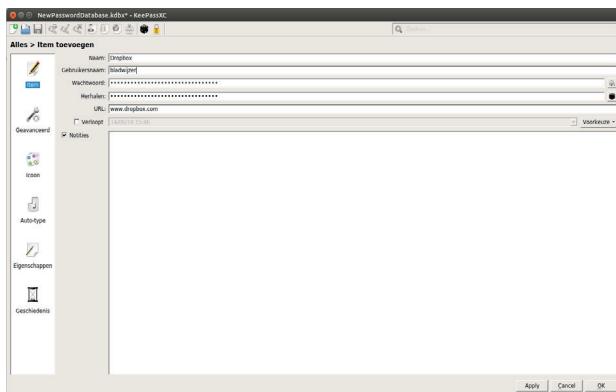
- Na het opslaan van de lege wachtwoordendatabank zal KeePassXC in een nieuw menu vragen om een 'Hoofdsleutel' in te stellen. Let wel: een wachtwoordmanager maakt het beheer van je wachtwoorden enkel veiliger als je hoofdwachtwoord voldoende sterk is.⁴

- Het wachtwoord dat we hier als voorbeeld gebruiken is 'Amvddstmozs1605!'. Het is een afgeleide van het spreekwoord 'Als men van de duivel spreekt, trapt men op zijn staart' met de toevoeging van een willekeurig cijfer '1605' en een '!'. Een computer zou er volgens de website howsecureismypassword.net een triljoen jaar over doen om het te kraken. Dat wachtwoord geef je in als hoofdwachtwoord. Het zal gebruikt worden om alle andere wachtwoorden te versleutelen in het databankbestand.

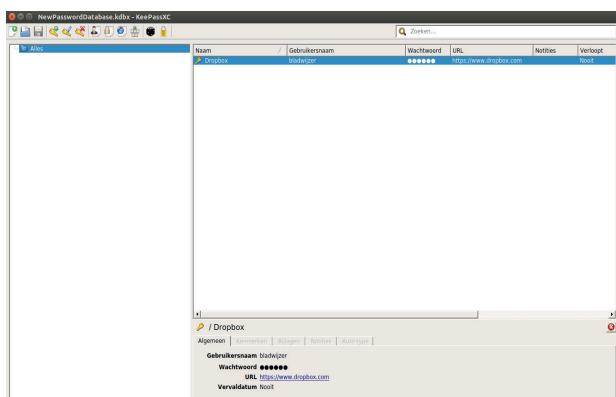


- Na het aanmaken en versleutelen van je wachtwoordendatabank, kun je starten met wachtwoorden toe te voegen. Druk daarvoor op het icoontje van de sleutel met de groene pijl naar beneden.

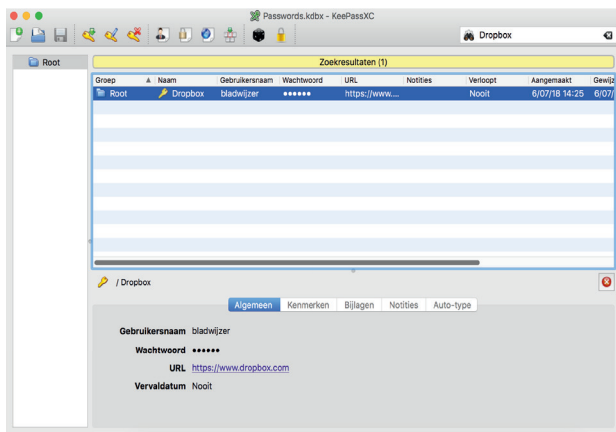




- Nieuwe wachtwoorden worden in het volgende scherm aangemaakt. Druk daarna op 'Apply' of 'Ok' en sla de wijzigingen op door in het menu via 'Database' op 'Database Opslaan' te klikken.



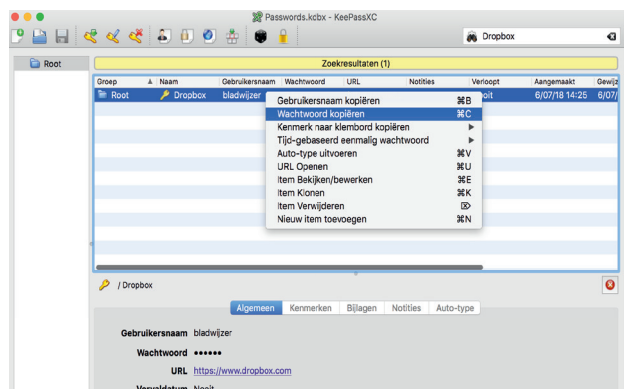
- Zo ziet de gebruikersinterface van KeePassXC eruit na het opslaan van een wachtwoord. Hoe meer informatie je invult, hoe beter je later in je opgeslagen wachtwoorden kunt zoeken.



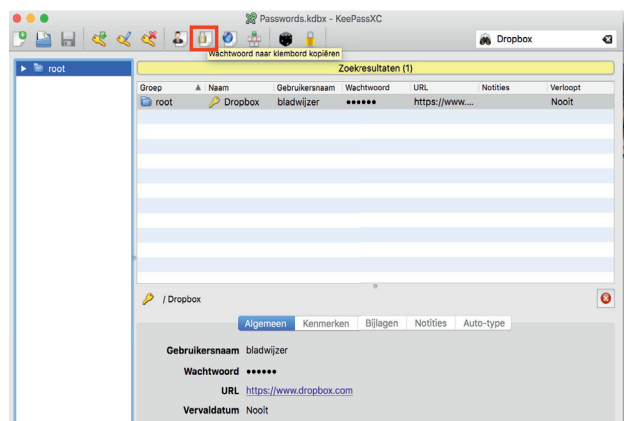
- Als je je wachtwoord wil gebruiken, dan zoek je het op in de databank. Je kan zoeken op ieder veld dat je ingevuld hebt.

De wachtwoordendatabank wordt opgeslagen in een .kdbx-formaat op je computer of op een USB-stick. Het is een goed idee om zowel een kopie op te slaan op de computer die je dagelijks gebruikt als een kopie op een externe harde schijf als back-up. Die back-up vul je best regelmatig aan met de laatste nieuwe wachtwoorden die je hebt aangemaakt. Zo voorkom je dat je back-up niet verouderd raakt.

Je kunt het .kdbx-formaat met je hoofdsleutel ook openen op andere computers waarop KeePassXC geïnstalleerd werd. Onderstaande screenshots werden zo gemaakt op een Apple computer met macOS als besturingssysteem.

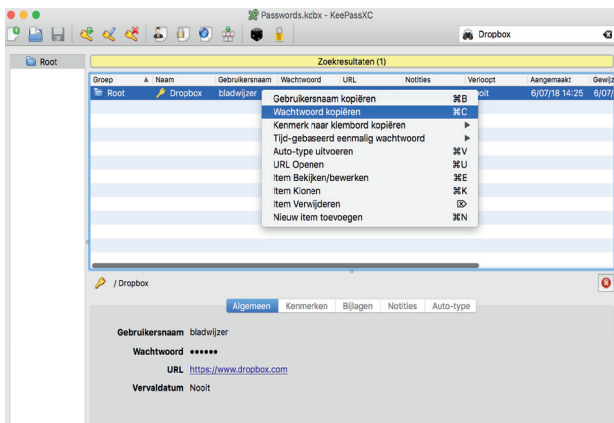


- Wanneer je je wachtwoord wil gebruiken, kan je dat zoeken in de wachtwoordendatabank. Je kunt zoeken op ieder veld dat je ingegeven hebt. Hier zoeken we op de naam die we aan het wachtwoord gegeven hebben.

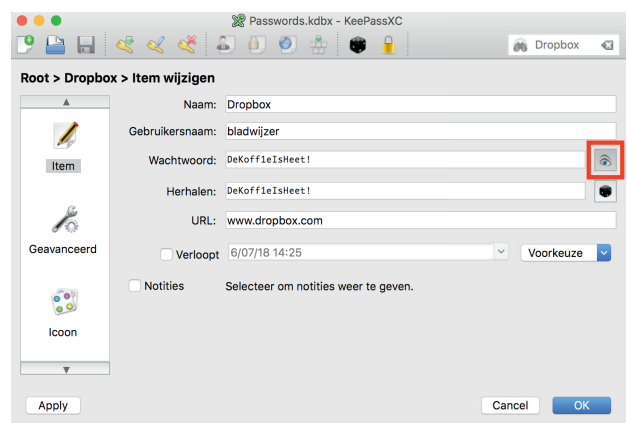


- Je gebruikersnaam vind je onder 'Gebruikersnaam'. Je wachtwoord kun je op verschillende manieren kopiëren:

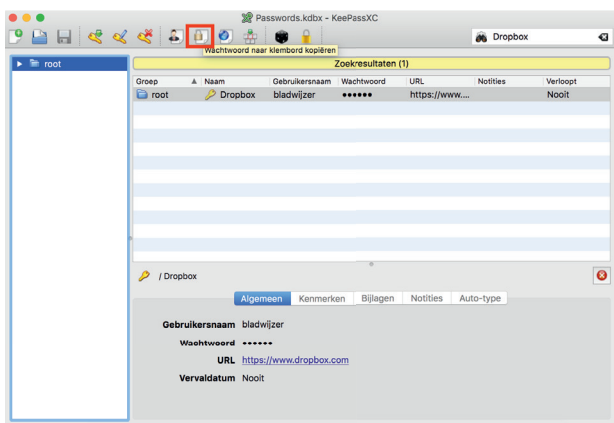
- door middel van een rechtermuisklik en 'Wachtwoord kopiëren' te selecteren;



- Door op het oog naast het veld met 'Wachtwoord' te klikken, krijg je je wachtwoord te zien.



- door op het blad met slot (achtste icoon van links) te klikken;



- Met die gegevens is het vervolgens mogelijk om je aan te melden op Dropbox.

Aanmelden

of een account maken



of

bladwijzer

.....

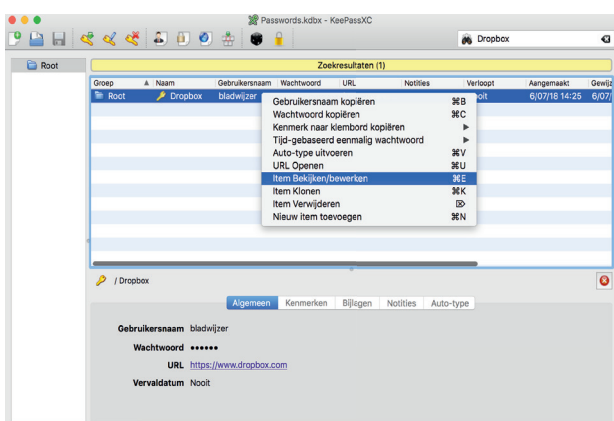
Deze pagina is beveiligd met reCAPTCHA en onderworpen aan het [Privacybeleid](#) en de [Servicevoorwaarden](#) van Google.

☒ Mijn gegevens onthouden

Aanmelden

[Wachtwoord vergeten?](#)

- of je kunt kiezen voor 'Item Bekijken/bewerken'. Je krijgt dan een detail van het volledige record te zien.



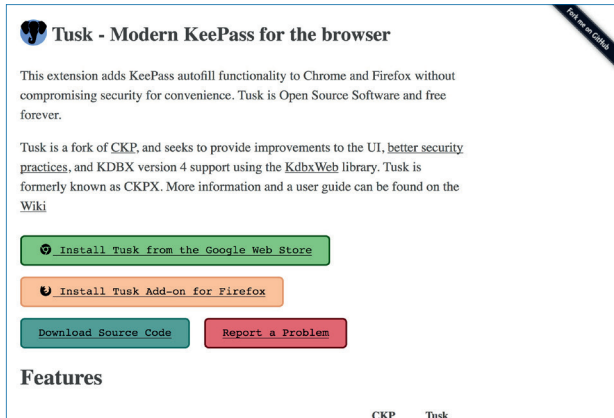
6. BEKNOPTE HANDLEIDING VOOR HET GEBRUIK VAN TUSK, DE BROWSERVARIANT VAN KEEPASS

Het voordeel aan KeePass is dat je de databank op verschillende platformen kan gebruiken.

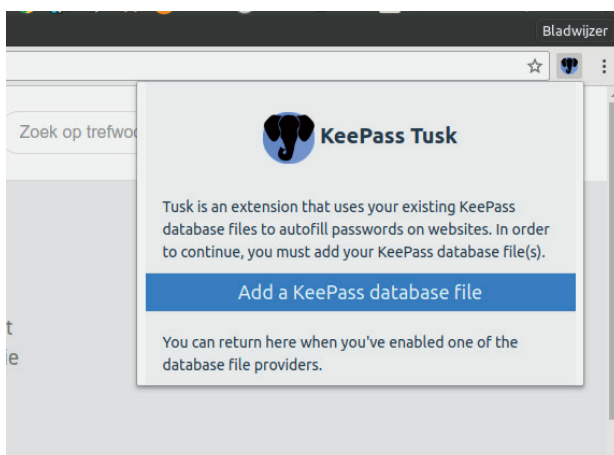
Voor wachtwoorden die je online gebruikt, is de browservariant Tusk de eenvoudigste oplossing. Het is een versie van KeePass die werd ontwikkeld voor de webbrowsers Chrome en Firefox en werkt als een extensie/add-on. De software laat toe om je eerder aangemaakte wachtwoordendatabankbestand (.kdbx) te openen in je webbrowser. Zo is het mogelijk om bijvoorbeeld wachtwoorden gemakkelijk in te vullen op loginpaginas van je internetaccounts.

6.1. Download en installeer Tusk

Je kan Tusk downloaden via <https://subdavis.com/Tusk/>. Je zult worden doorgestuurd naar de officiële extensie/add-on-websites van Firefox of Chrome.

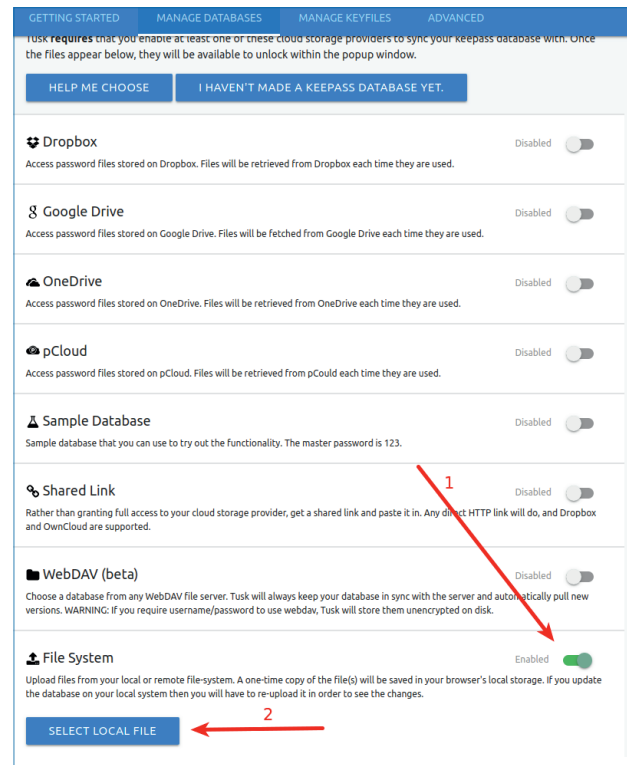


6.2. Voeg je wachtwoordendatabank toe



Het eerste dat moet gebeuren is je (zoals hiervoren beschreven) aangemaakt databankbestand opladen in de Tusk-extensie. De eerste keer dat je Tusk opent, is dat het eerste dat je gevraagd wordt. Klikken op 'Add a KeePass database file' brengt je in de instellingen van de extensie.

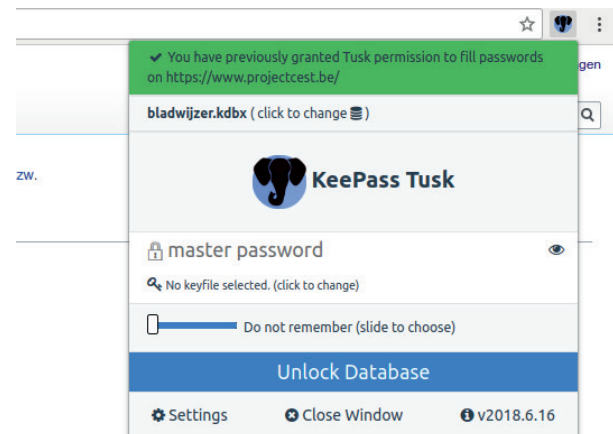
- Er zijn verschillende locaties beschikbaar vanwaar je jouw wachtwoordendatabank kunt opladen. In dit voorbeeld selecteer je de laatste optie om het .kdbx-bestand van je computer op te laden en te gebruiken via de browserextensie.
- Je zult vervolgens zien dat wanneer je terug op het Tusk-icoontje klikt, je de vraag krijgt om het bestand met de wachtwoordendatabank dat je net hebt opgeladen, te ontgrendelen.



6.3. ONLINE GEBRUIK VAN JE WACHTWOORDENDATABANK



- Wanneer je naar een website gaat waarvoor je een wachtwoord hebt opgeslagen en op Tusk klikt om de gegevens in te vullen, zal de webbrowser een melding weergeven om de extra rechten die de extensie heeft gevraagd wel of niet te aanvaarden.

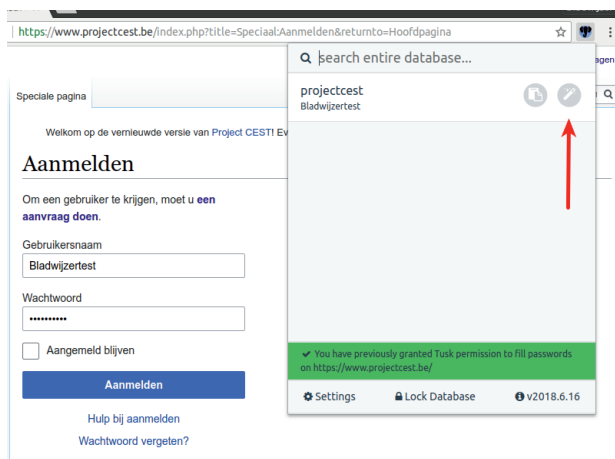


- Door op 'Toestaan' te klikken zal Tusk de wachtwoorden aanvullen. Wanneer je op 'Weigeren' klikt, zal dat betekenen dat je de gegevens zelf moeten handmatig plaatsen bij de loginpagina's.
- Als je naar een website surft waarvoor je wachtwoorden hebt opgeslagen en je hebt de extra rechten geaccepteerd, zul je zien dat Tusk het betreffende wachtwoord vindt. De gebruikersnaam en wachtwoord zal worden ingevuld in de loginvelden

op de website als je op de knop klikt met het icoontje van een toverstokje.

Zoals wel vaker bij computers gaat niks boven de ervaring. Meer dan dit artikel opnieuw te lezen en te wachten tot je alles begrijpt, raden we je aan om aan de slag te gaan. Je zal merken dat wat theoretisch moeilijk lijkt, in de praktijk veel gemakkelijker is. We hopen in ieder geval dat we langs deze weg allen veiliger omgaan met de informatie die ons zo dierbaar is.

Lode Scheers, PACKED vzw
Nastasia Vanderperren, PACKED vzw
en Rony Vissers, PACKED vzw



¹ Voor meer info, zie <https://www.safeonweb.be/nl/gebruik-sterke-wachtwoorden>

² KeePass is de originele versie die in 2003 gepubliceerd werd en enkel voor Windows kan worden gebruikt. Nadien is de code door het KeePassX-team gebruikt om een versie te maken voor Linux. Later werd KeePassXC ontwikkeld om ook Mac Os X te ondersteunen. De stabiele versie werd in mei 2018 gepubliceerd en ondersteunt nu zowel Mac Os X, Windows als Linux.

³ Een overzicht van de eigenschappen van noemenswaardige wachtwoordmanagers kun je vinden op https://en.wikipedia.org/wiki/List_of_password_managers#Comparison

⁴ Een hoofdsleutel verzinnen die niet alleen sterk en veilig maar ook gemakkelijk te onthouden is, is eenvoudig als je gebruik maakt van gezegdes, spreekwoorden of weerspreuken. Kies een zin van minimum acht woorden. Neem de eerste letter van elk woord, en maak van een letter in je wachtwoord (bv. de eerste) een hoofdletter. Voeg er vervolgens minimaal vier cijfers en een leesteken aan toe. De volgorde is niet belangrijk. Zo kom je aan het minimum van dertien karakters. Bij de keuze van het wachtwoord, zijn de enige belangrijke criteria voldoende lengte, en het gebruik van hoofdletters, kleine letters, cijfers, symbolen en leestekens. Het is nog beter als je een zin gebruikt in combinatie met cijfers en leesteken(s), maar dat is minder snel in gebruik. Als je wil weten hoe sterk je wachtwoord is, test je wachtwoord dan uit op de website howsecureismypassword.net.