

Uw PC, Tablet en Telefoon veilig gebruiken.

- Geen enkel apparaat verbonden met het internet is 100 % veilig.
- We kunnen wel proberen het moeilijk te maken voor ongewenste bezoekers om binnen te komen.
- De standaard middelen tegen ongewenst bezoek zijn wachtwoorden en pin codes.
- De effectiviteit van een wachtwoord wordt hoofdzakelijk bepaald door de lengte.
- Authenticatie in twee stappen biedt een sterk verbeterde veiligheid, bekend als 2FA.

Uw PC, Tablet en Telefoon veilig gebruiken.

- Voor veel websites en webwinkels moet je je registreren en inloggen met een wachtwoord.
- Geef bij de registratie alleen de strikt noodzakelijke informatie.
- Hoe veilig zijn uw gegevens daar opgeslagen?
- Bedenk dat aanbieders van gratis diensten ook een verdienmodel hebben en dat is vaak de verkoop van uw gegevens.

Uw PC, Tablet en Telefoon veilig gebruiken.

- Goed beveiligde websites en webdiensten slaan wachtwoorden altijd versleuteld op. Er wordt een unieke hash-code gegenereerd die uit 32, 34 of meer karakters bestaat, afhankelijk van de gebruikte algoritme.
- De hash lengte is onafhankelijk van de lengte van het wachtwoord.
- Uit deze hash code is het originele bestand of wachtwoord niet meer terug te rekenen.
- Bekende technieken zijn MD5, SHA-1 en SHA-256.

Uw PC, Tablet en Telefoon veilig gebruiken.

- Een leuk experiment is om met een online dienst zelf een hash code te genereren.
- Ga naar: <https://www.md5hashgenerator.com/>
- Vul daar een wachtwoord in waarvan je een hash code wilt hebben.
- Schrijf de gegenereerde hash op.
- Verander één karakter in het wachtwoord en genereer nogmaals een hash.
- Zie je het verschil?

Uw PC, Tablet en Telefoon veilig gebruiken.

- Vaak hoor je dat er weer een website is gekraakt en dat er miljoenen wachtwoorden zijn buit gemaakt.
- Dat is meestal onjuist niet de wachtwoorden maar de hash codes zijn gestolen.
- Kan men daar wat mee, ja door simpel van miljoenen wachtwoorden de hash te genereren en te testen of de hash overeenkomt met één van de gestolen hashes.
- Men gebruikt hiervoor de Rainbow tables, een verzameling van al bekende en gebruikelijke wachtwoorden.
- Hier komt het belang van een lang wachtwoord naar voren.

Uw PC, Tablet en Telefoon veilig gebruiken.

- Een lang willekeurig wachtwoord is met de rainbow tables veel moeilijker te kraken.
- Een zeer snelle PC met moderne GPU kan wel tot één miljard wachtwoorden per seconde genereren, hashen en vergelijken.
- Een wachtwoord van 20 karakters heeft 72 tot de macht 20 mogelijke combinaties. Dat levert het volgende getal op:

14.016.833.953.562.607.293.918.185.758.734.155.776
- De gebruikte computer is al versleten voordat een klein deel van de combinaties is geprobeerd.

Uw PC, Tablet en Telefoon veilig gebruiken.

- Maar lange wachtwoorden kunnen wij slecht onthouden.
- We kunnen een wachtwoord zin gebruiken, bijv.

[Natuurgebied de Rottige Meenthe.](#)

Dit wachtwoord bestaat inclusief spaties uit 32 karakters, voldoende lang.

- We moeten wel voor allerlei diensten verschillende wachtwoorden gebruiken, dat wordt dan wel weer lastig. Hierbij kan ons een wachtwoord manager helpen. In de volgende dia's kijken we naar Keepass.

Uw PC, Tablet en Telefoon veilig gebruiken.

- Keepass is een lokale wachtwoord manager die op je PC, Tablet of Smartphone geïnstalleerd wordt.
- Keepass gebruikt een met AES256 versleutelde database van de opgeslagen wachtwoorden.
- De database kan op een USB stick worden opgeslagen.
- Dat betekent dat zonder de USB stick Keepass niet gebruikt kan worden.
- Combineer de Keepass database met Rohos Logon op de USB stick en er is alleen toegang tot de PC met de USB stick.

Uw PC, Tablet en Telefoon veilig gebruiken.

- Keepass installeren.
- Download Keepass van: <https://keepass.info/>
- Kies de meest recente stabiele versie.
- Op de site zie je ook nog een hele reeks uitvoeringen bestemd voor andere apparaten.
- Naast deze officiële uitvoering zijn er een aantal forks, bijvoorbeeld KeepasX. Iets eenvoudiger van opzet. De databases zijn uitwisselbaar.

Uw PC, Tablet en Telefoon veilig gebruiken.

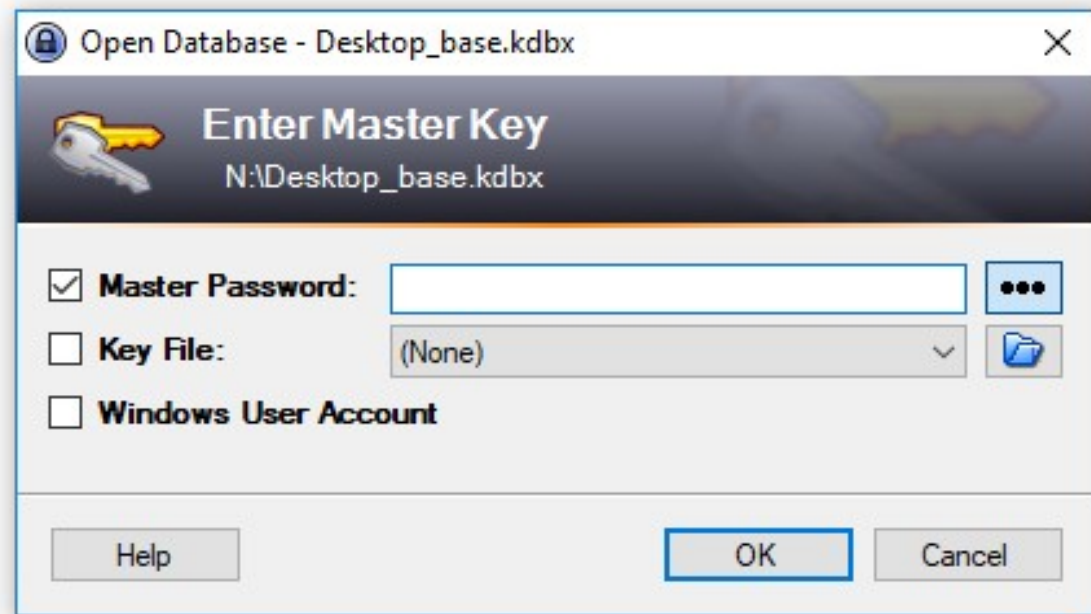
- Nadat je Keepass geïnstalleerd hebt wordt er bij de eerste start van het programma een venster geopend waarin gevraagd wordt een database naam in te vullen.
- Het database bestand krijgt de extensie .kdbx.
- Kies voor de opslag locatie een USB stick.
- Installeer ook Rohos Logon Free. Download van: <https://www.rohos.com/products/rohos-logon-free/>
- Het is met de Rohos logon key mogelijk ook voor het inloggen op je PC een lang wachtwoord te kiezen.

Uw PC, Tablet en Telefoon veilig gebruiken.

- Nadat je de nieuw te vormen database een naam hebt gegeven en de opslag locatie hebt ingesteld klik je op Save.
- Een nieuw venster opent waarin je het master wachtwoord moet invullen. Dit wachtwoord of wachtwoordzin moet moeilijk te kraken zijn. Dat is heel belangrijk!! Hiervan hangt de hele veiligheid van het systeem vanaf. Klik op OK.
- In het venster wordt ook de kwaliteit van je wachtwoord getoond d.m.v. een balk. Een groen uiteinde is goed.
- Als je het wachtwoord vergeet is het uit met de pret, er is geen enkele mogelijkheid om bij je wachtwoorden te komen.

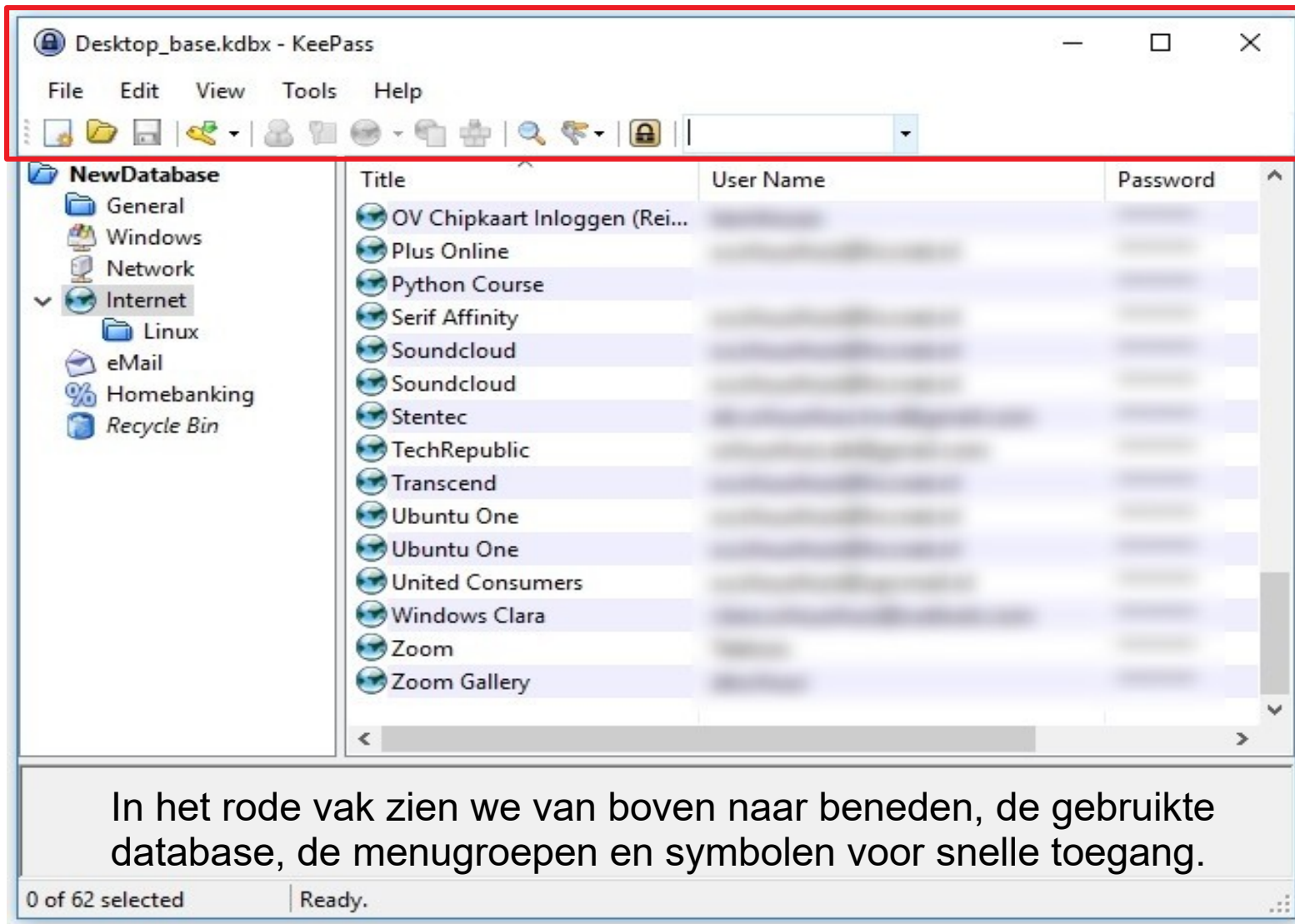
Uw PC, Tablet en Telefoon veilig gebruiken.

- Als je Keepass opstart d.m.v. een klik op het icoontje  verschijnt het inlogvenster.

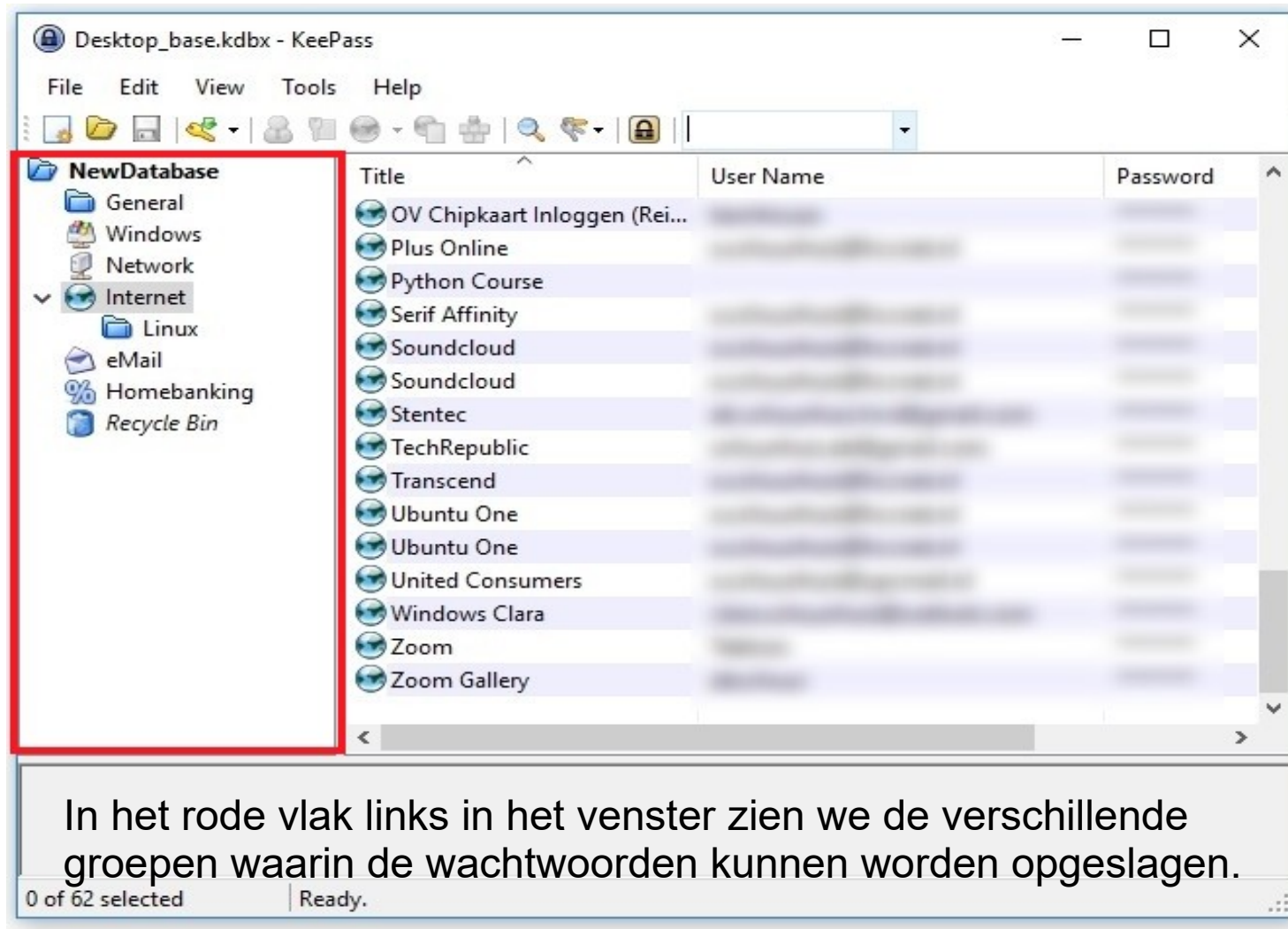


Vul het wachtwoord in en controleer met het vak met de drie stipjes of het correct is ingevuld. Ja? Klik op OK. Een nieuw venster opent waarin je toegang hebt tot de in de database opgeslagen wachtwoorden.

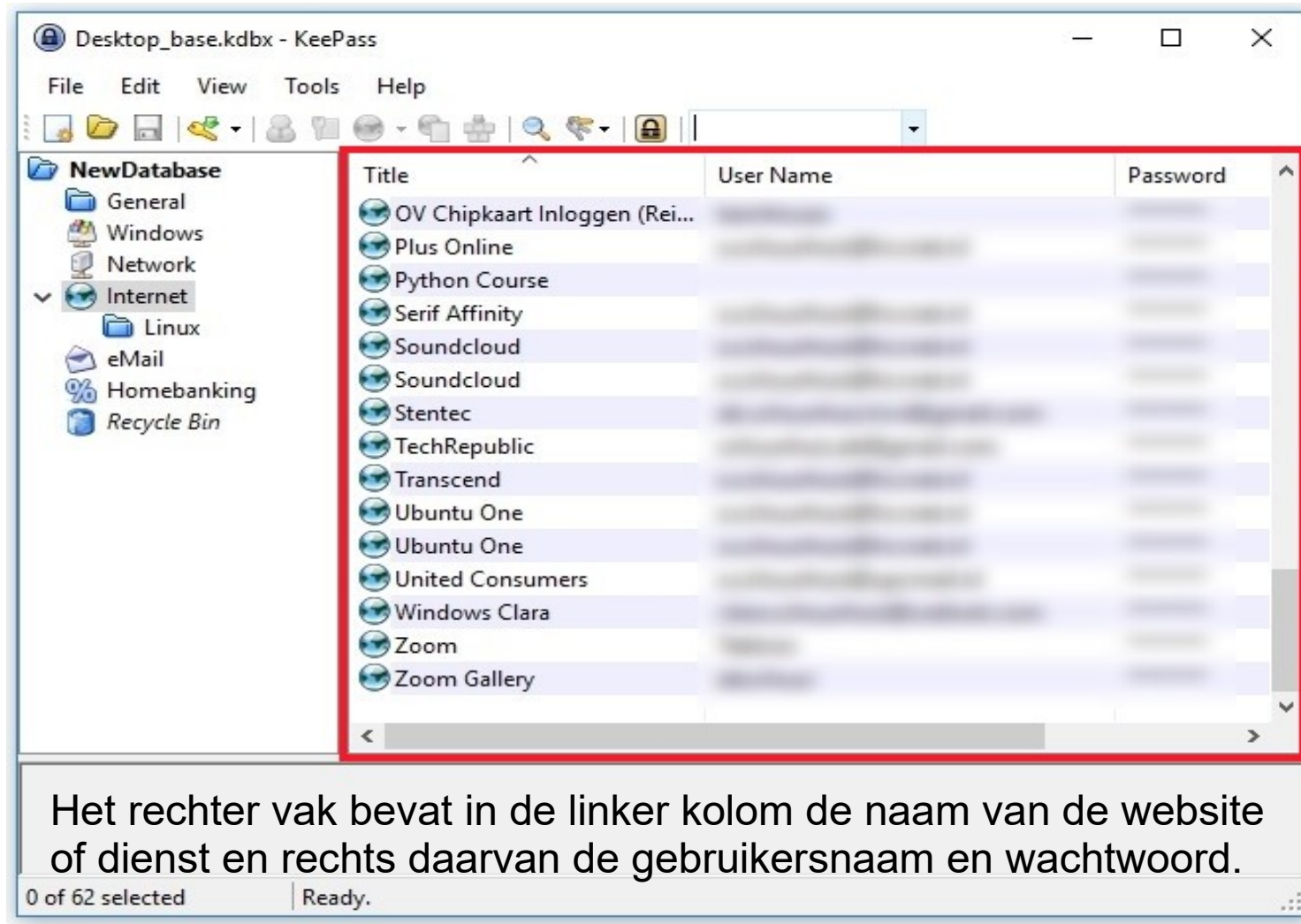
Uw PC, Tablet en Telefoon veilig gebruiken.



Uw PC, Tablet en Telefoon veilig gebruiken.

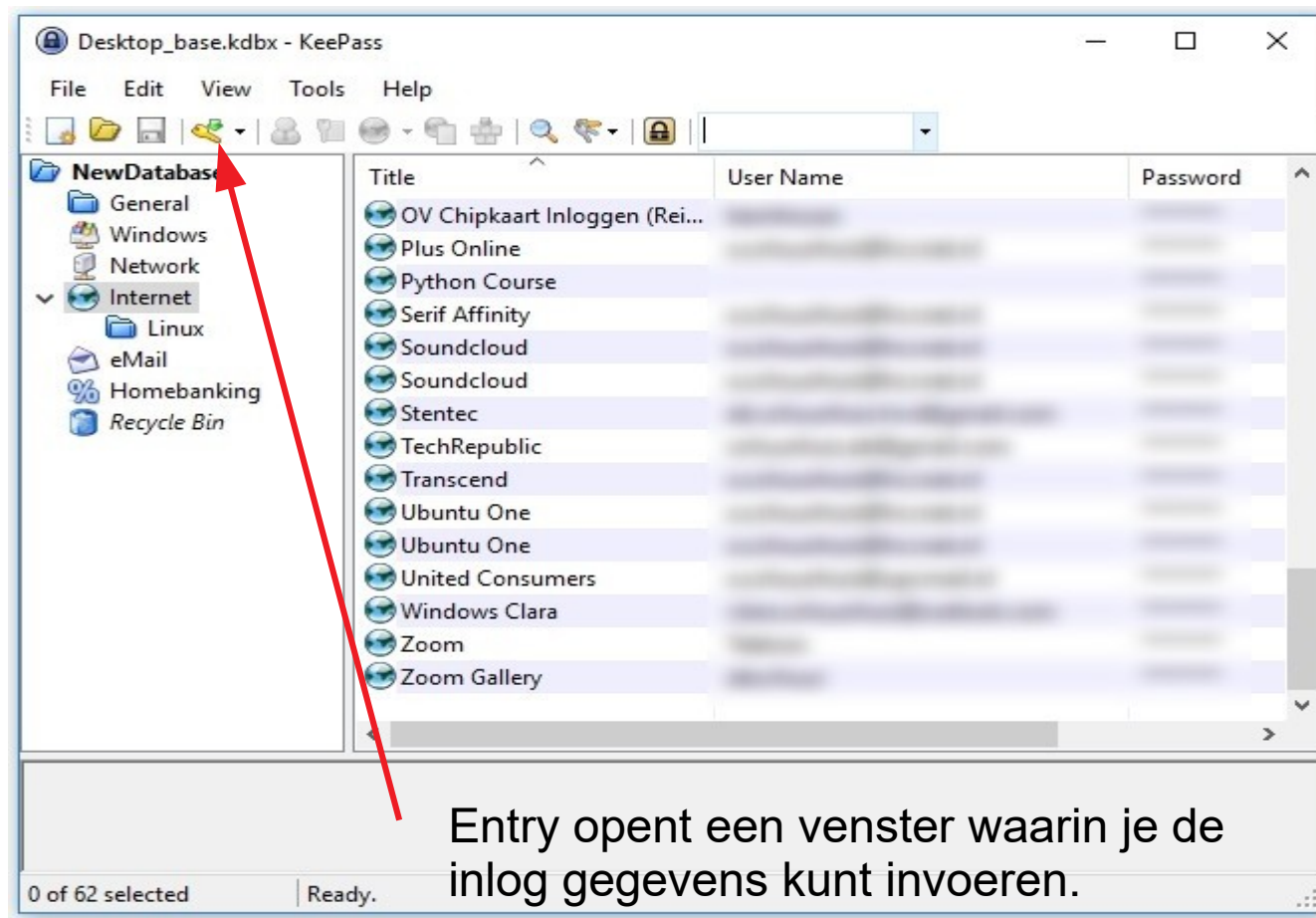


Uw PC, Tablet en Telefoon veilig gebruiken.



Uw PC, Tablet en Telefoon veilig gebruiken.

- Om een nieuw wachtwoord en gebruikersnaam in te voeren klik je op het Entry symbool.



Uw PC, Tablet en Telefoon veilig gebruiken.

Add Entry
Create a new entry.

Entry | Advanced | Properties | Auto-Type | History

Title: Icon:

User name:

Password:

Repeat:

Quality: 110 bits 20 ch.

URL:

Notes:

Title: bijvoorbeeld HCCnet
Username: uw gebruikersnaam
Password: uw eigen bedacht of toegewezen wachtwoord of een door KeePass gegenereerd wachtwoord.


☐ Expires: 6- 1-2018 00:00:00

Tools OK Cancel

Uw PC, Tablet en Telefoon veilig gebruiken.

- Als je voor het registreren op een website zelf een gebruikersnaam en wachtwoord moet bedenken, is het handig om het wachtwoord door KeePass te laten genereren.
- Keepass levert standaard zeer sterke wachtwoorden met 20 karakters.
- De procedure is als volgt: start Keepass, klik op New Entry, vul de naam van de website, en de gebruikersnaam in en gebruik het reeds ingevulde wachtwoord. Klik op OK.

Uw PC, Tablet en Telefoon veilig gebruiken.

- Vervolgens ga je naar het registratiescherm van de dienst of website waarvoor je je wilt registreren.
- Selecteer in het nog geopende Keepass scherm de zojuist ingevoerde website of dienst.
- Klik op het gebruikersnaam symbool  , de gebruikersnaam wordt nu naar het klembord gekopieerd.
- Klik nu rechts in het gebruikersnaamvak van het registratiescherm. Het context menu opent en klik op plakken. De gebruikersnaam is nu ingevoerd.
- Herhaal de procedure voor het wachtwoord. Klik op het sleutel symbool  . Het wachtwoord is nu naar het klembord gekopieerd. Plak het wachtwoord in het vakje voor het wachtwoord. Klik op OK.

Uw PC, Tablet en Telefoon veilig gebruiken.

Add Entry
Create a new entry.

Entry | Advanced | Properties | Auto-Type | History

Title: Icon:

User name:

Password:

Repeat:

Quality: 110 bits 20 ch.

URL:

Notes:

Standaard

☐ Expires: 6- 1-2018 00:00:00

Tools OK Cancel

Je hebt ook nog keuze in het formaat en karakter set van het te genereren wachtwoord.

- (Baseren op een vorig wachtwoord)
- (Automatisch gegenereerde wachtwoorden voor nieuwe invoer)
- Hex Key - 40-Bit (ingebouwd)
- Hex Key - 128-Bit (ingebouwd)
- Hex Key - 256-Bit (ingebouwd)
- Willekeurig MAC-adres (ingebouwd)

Door op de drie puntjes naast het wachtwoord te klikken zie je het gegenereerde wachtwoord.

Uw PC, Tablet en Telefoon veilig gebruiken.

Nieuwe invoer

Nieuwe wachtwoordinvoer aan de database toevoegen.

Invoer Geavanceerd Eigenschappen Auto-typen Geschiedenis

Titel: Pictogram:

Gebruikersnaam:

Wachtwoord:

Herhaal:

Kwaliteit: 127 bits 32 tk.

URL:

Opmerkingen:

☐ Vervaldatum: 29-10-2018 00:00:00

Extra OK Annuleren

Hex Key 128 bit genereert een wachtwoord met 32 hexadecimale tekens, 0 – 9, a – f.

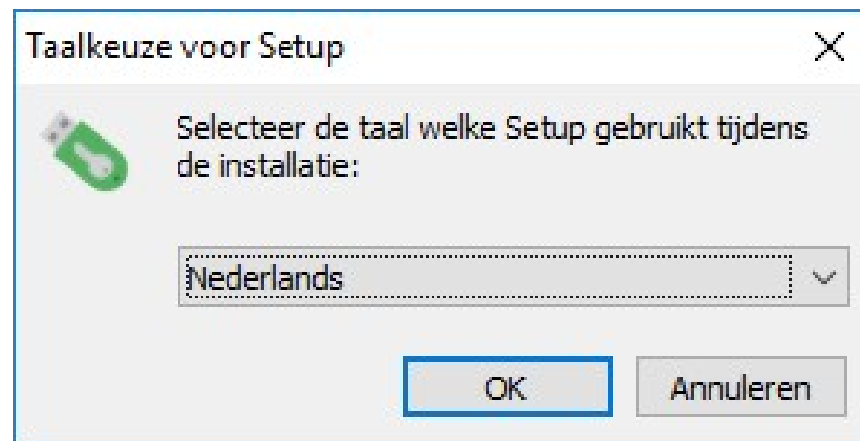
Uw PC, Tablet en Telefoon veilig gebruiken.

- Om helemaal zeker te zijn dat je ook bij crash van je harddisk of verlies van je USB stick nog de beschikking hebt over je Keepass database kun je een backup in de cloud plaatsen.
- Gebruik je Thunderbird als email programma, dan kun je met Mozbackup een backup maken.

Mozbackup maakt een complete backup van al je berichten, adresboek en instellingen. Plaats de backup hiervan ook in de Cloud.

Uw PC, Tablet en Telefoon veilig gebruiken.

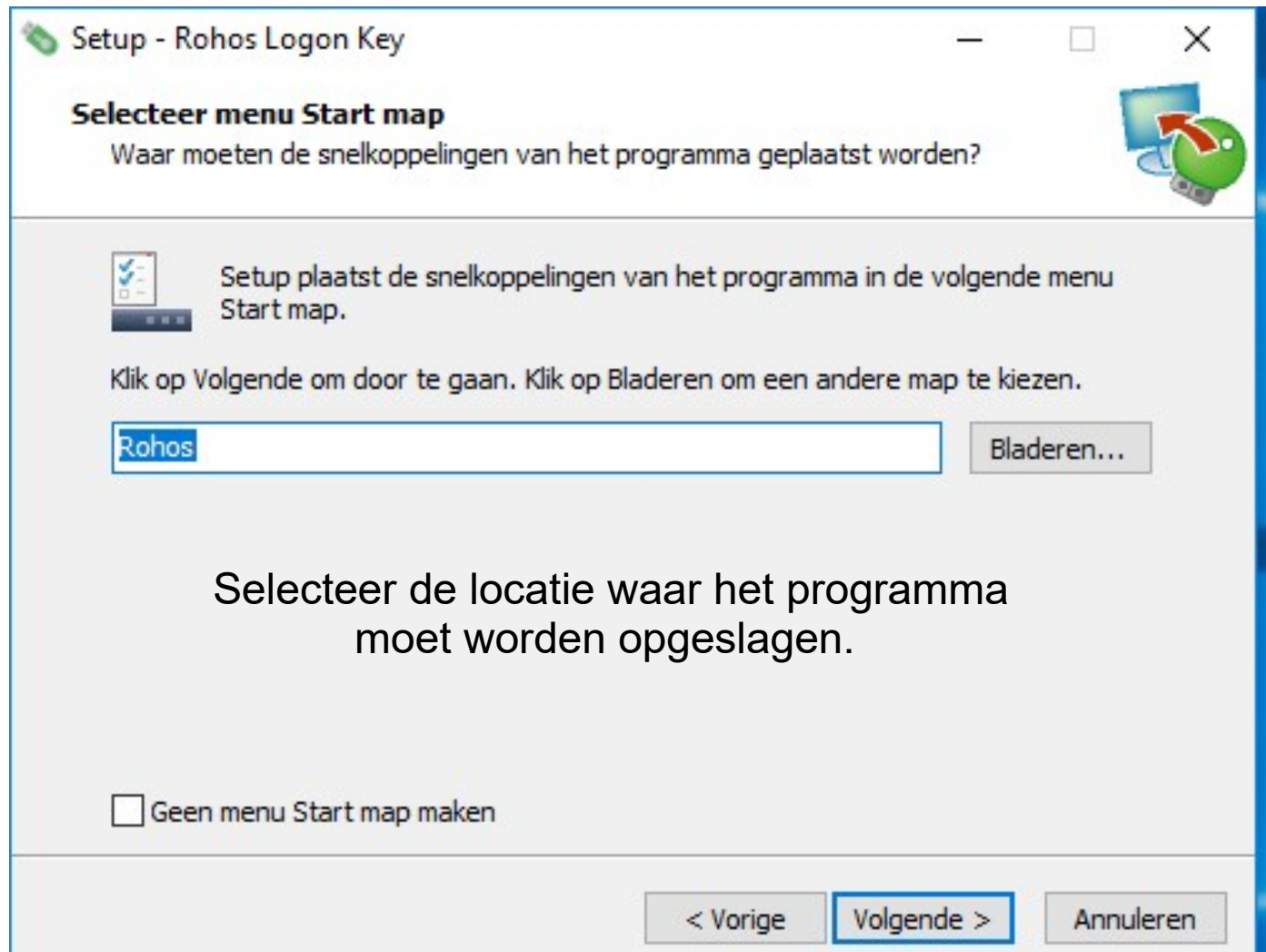
- Rohos Logon Free installeren.
- Download Rohos Logon van:
- <https://www.rohos.com/products/rohos-logon-free/>
- Start het gedownloade bestand: rohos-logon-free.exe
- Je krijgt nu eerst de taalkeuze.



Uw PC, Tablet en Telefoon veilig gebruiken.



Uw PC, Tablet en Telefoon veilig gebruiken.

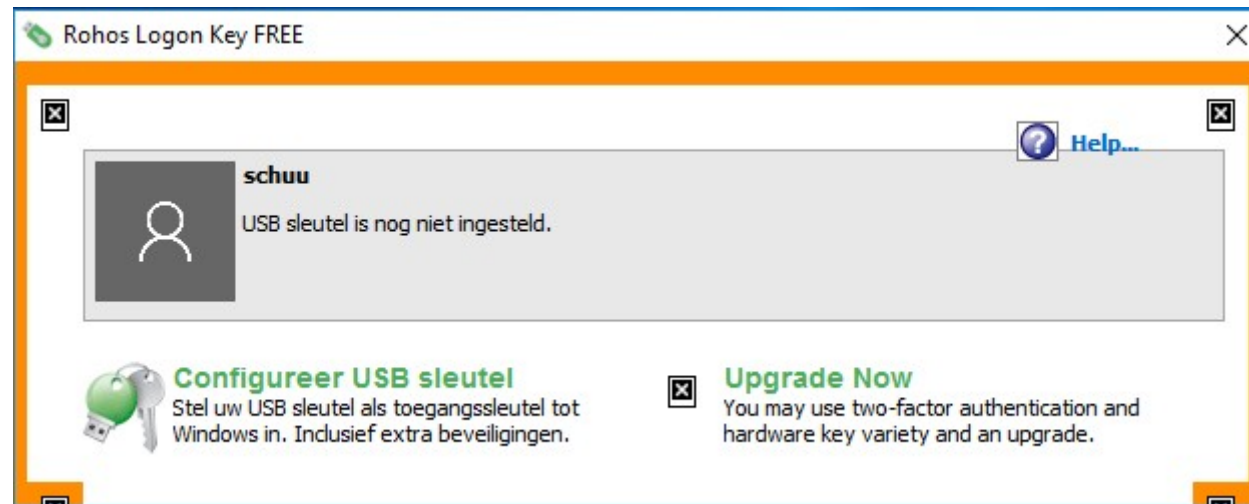


Uw PC, Tablet en Telefoon veilig gebruiken.



Uw PC, Tablet en Telefoon veilig gebruiken.

- Configuratie van de USB sleutel.



Klik op Configureer USB sleutel om het configureren te starten.

Uw PC, Tablet en Telefoon veilig gebruiken.



Vul uw wachtwoord in en klik daarna op: USB sleutel instellen.
Rohos probeert het wachtwoord te verifiëren. Als u er zeker van bent dat het wachtwoord correct is kunt u eventuele waarschuwingen negeren.

Uw PC, Tablet en Telefoon veilig gebruiken.

- Beheerstaken scheiden van dagelijks werk op uw computer.
- Maak een apart werk account aan, en geeft dit account beperkte rechten. Hiermee voorkom je dat per ongeluk malware wordt geïnstalleerd.
- Gebruik het beheerders account alleen voor beheerstaken.
- Gebruik voor beide accounts verschillende wachtwoorden.

Uw PC, Tablet en Telefoon veilig gebruiken.

- Inloggen met Facial Recognition (Gezichtsherkenning).
- Om Facial recognition te kunnen gebruiken heb je een PC met een webcam nodig. De kwaliteit en de resolutie van de camera moet voldoen aan de eisen van het programma.
- De prijzen lopen uiteen van ca. 15 tot honderden euro's. Dit is onder meer afhankelijk van de gestelde eisen m.b.t. veiligheid, nauwkeurigheid en het aantal personen dat herkend moeten worden.
- Rohos biedt een programma aan voor € 17. Er is een trial voor 15 dagen.
<https://www.rohos.com/products/rohos-face-logon/>

Uw PC, Tablet en Telefoon veilig gebruiken.

- Vinger afdruk scanners aangesloten op een USB poort maken het mogelijk zonder wachtwoord in te loggen. Zie voorbeelden.
- Veel smartphones bieden een ingebouwde FP scanner.
- De FP scanner kan ook gebruikt worden voor 2 factor authenticatie. Onder andere bij Google.



Renkforce
Conrad



Alibaba China

Prijzen variëren tussen 11 en 30 euro.

Uw PC, Tablet en Telefoon veilig gebruiken.

- Twee stappen authenticatie. (2FA)
- Het principe gaat uit van: iets dat U weet, bijvoorbeeld gebruikersnaam en wachtwoord. (Stap één) en iets dat u hebt, bijvoorbeeld een smartphone, een FP scanner, een Yubikey of een ander token.
- Verificatie vindt dan plaats d.m.v. een SMS met een verificatiecode die moet worden ingevuld. Of door het uitlezen van de FP scanner of Yubikey
- Google biedt standaard 2FA aan. Dat kan via een SMS of een prompt naar uw telefoon. Ook een USB token is mogelijk.

Uw PC, Tablet en Telefoon veilig gebruiken.

- In het betalingsverkeer (internet bankieren) wordt vaak gebruik gemaakt van een hardware token generator. Voorbeelden hiervan zijn de e-identifier van ABNAMRO en de RABO Scanner.
- ING bank gebruikte TAN codes (Transaction Authentication Number) en is onlangs overgestapt op de PAC codes (Personal Authentication Code).
- De communicatie tussen U en de bank mag dan goed beveiligd zijn, het grootste gevaar zit toch tussen de stoel en het beeldscherm. Controleer altijd of het giro of bankrekeningnummer waarnaar u geld overmaakt klopt.

Uw PC, Tablet en Telefoon veilig gebruiken.

- Er wordt aan nog veiliger inlog technieken gewerkt.
- Hierbij wordt een lang wachtwoord in stukjes gehakt en vervolgens versleuteld opgeslagen op verschillende servers.
- De servers moeten samen m.b.v. een bepaald protocol het wachtwoord verifiëren. Geen van de servers krijgt ooit het hele wachtwoord te zien. Een hack van één enkele server levert dus geen gevaar op.

Uw PC, Tablet en Telefoon veilig gebruiken.

- Demo Keepass installeren en configureren.

- Stappen:

Keepass installeren.

Bepalen waar de database *.kdbx wordt opgeslagen.

- Master password instellen.
- Inlog gegevens in de database invoeren.

Uw PC, Tablet en Telefoon veilig gebruiken.

- Phishing. Voorbeeld van een phishing mail.



Geachte klant,

Ter bescherming wordt uw Apple ID automatisch vergrendeld.

We hebben een ongeautoriseerde aanmeldingspoging naar uw Apple ID gedetecteerd vanaf een andere IP-locatie. Werk uw informatie snel bij, zodat u kunt:

Aanmeldingsdatum: 23 juni, 2018

Locatie: Mongolië

Besturingssysteem: Windows 8

Browser: Google Chrome

Verifieer vandaag nog uw identiteit of uw account zal worden uitgeschakeld.

Wijzig daarna uw appleid-wachtwoord. Om uw Apple ID te verifiëren, raden wij u aan naar:

[Login to Apple ID](#)

Met vriendelijke groet,
Apple

* De locatie is bij benadering en bepaald door het IP-adres dat het was

Deze e-mail kan geen antwoorden ontvangen. Ga voor meer informatie naar het Helpcentrum van Apple .

U hebt deze verplichte e-mailserviceaankondiging ontvangen om u op de hoogte te houden van belangrijke wijzigingen in uw Apple-product of -account.

Controleer altijd het email adres en verifieer per telefoon.

Uw PC, Tablet en Telefoon veilig gebruiken.

Er wordt momenteel veel gediscussieerd
Over de veiligheid van wachtwoorden.

Vaak is er ook twijfel over de veiligheid van
wachtwoord managers.

Er worden ook nieuwe methoden voorgesteld om
met wachtwoorden om te gaan. Getuige het
bijgaand filmpje.

Uw PC, Tablet en Telefoon veilig gebruiken.

Klik op onderstaande URL
en vervolgens op Example.

<http://www.safepasswords.org/>

Uw PC, Tablet en Telefoon veilig gebruiken.

Voorbeeld van met drie woorden wachtwoord herinneren.
Gebruik drie woorden met zoveel mogelijk letters uit het alfabet.

Handeling – brulboei – ijzeroxide (aanvulling: H8%c)

Procedure: kijk waar de letter uit site naam waarvoor een wachtwoord ingevuld moet worden het eerst voorkomt in de drie woorden en neem dan de volgende letter. Komt de letter niet voor neem dan een standaard vervangend karakter (wildcard), bijvoorbeeld \$.

Conrad → \$eduneH8%c

Alternate → ni\$ludn\$IH8%c

DigiDAb → enbelnrH8%c

Uw PC, Tablet en Telefoon veilig
gebruiken.

Vragen?