Flanders Computer Club

Flanders Nieuwsflash Bulletin

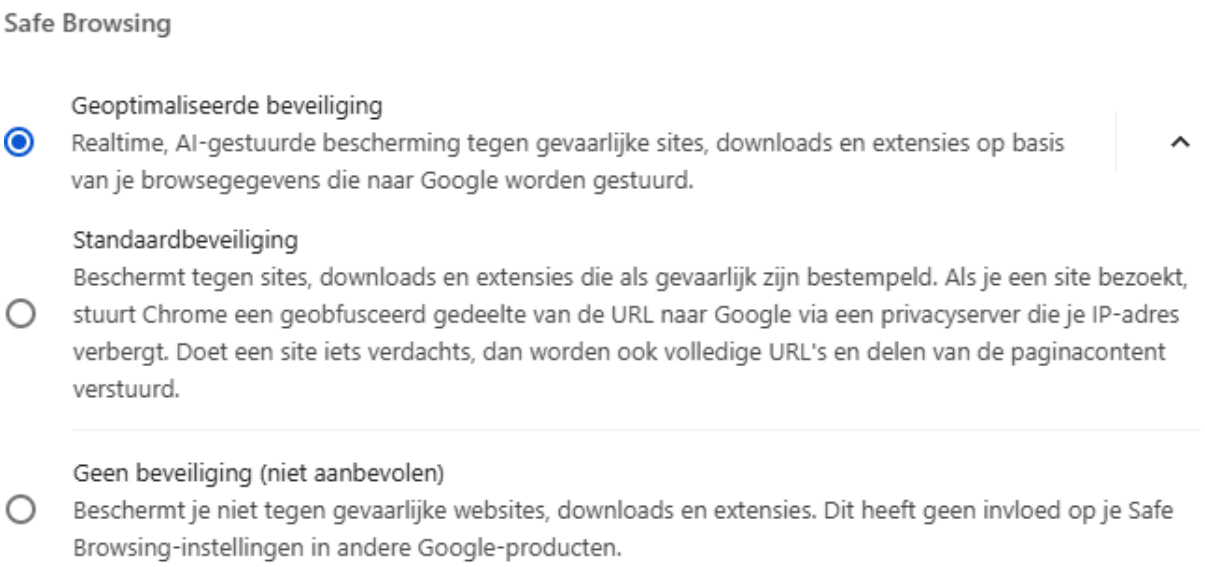
Werk jaar 41 – Editie: April 2026

Flanders Nieuwsflash Bulletin brengt maandelijks een overzicht van de artikels die verschenen zijn op onze website. Dit document is aangemaakt in een groter lettertype zodat het desgewenst kan afgedrukt worden als A5-boekje. Bezoek onze website voor de meest recente artikels.

www.flanderscomputerclub.be

BEVEILIGING – 24/04/2026
GOOGLE SAFE BROWSING

Google Safe Browsing beschermt gebruikers tegen schadelijke websites, malware, phishing en ongewenste software door het internet continu te scannen en onveilige URL's op lijsten bij te houden. Het waarschuwt gebruikers in Chrome, Firefox en Safari voordat ze een gevaarlijke site bezoeken of schadelijke bestanden downloaden.



Als je Safe Browsing aan hebt staan, dan krijg je een waarschuwing in je browser voordat je een gevaarlijke site bezoekt of een schadelijk bestand downloadt.
Je hebt een bescherming tegen bedreigingen. De tool detecteert en blokkeert phishing (*fraude*), malware (*schadelijke software*) en ongewenste software. Safe Browsing controleert websites in realtime en via de databases met bekende gevaren.
Je hebt als gebruiker de keuze uit Geoptimaliseerde beveiliging of Standaardbeveiliging. De eerste biedt de sterkste, proactieve bescherming, maar stuurt meer gegevens naar Google, terwijl de standaardbeveiliging een basisbescherming tegen bekende gevaren biedt.
Safe Browsing werkt zowel in Windows als in Android.

Werkwijze Windows:

- *Start Chrome*
- *Ga naar 'Instellingen' → 'Privacy en beveiliging' → 'Beveiliging'*
- *Maak een keuze tussen 'Geoptimaliseerde beveiliging' (aanbevolen) of 'Standaardbeveiliging'*

Werkwijze Android:

- *Open de Chrome-app*
- *Tik op de drie puntjes rechts en ga naar 'Instellingen'*
- *Tik op 'Google-services'*
- *Zet de schakelaar bij 'Zoekopdrachten en browsefunctionaliteit verbeteren' op aan (dit activeert de Safe Browsing-functionaliteit)*

Op je computer kan je ook een veiligheidscheck in Chrome uitvoeren met een ingebouwde tool die direct uw browserbeveiliging controleert op gehackte wachtwoorden, schadelijke extensies, de up-to-date status van Chrome en de actieve Safe Browsing-instellingen.

Werkwijze Windows:

- *Start Chrome*
- *Ga naar 'Instellingen' → 'Privacy en beveiliging' → 'Veiligheidscheck'*
- *Chrome controleert uw instellingen. Als er problemen zijn, klik je op het item om de instructies te volgen*

FVG
(Geraadpleegde bronnen: Google support)

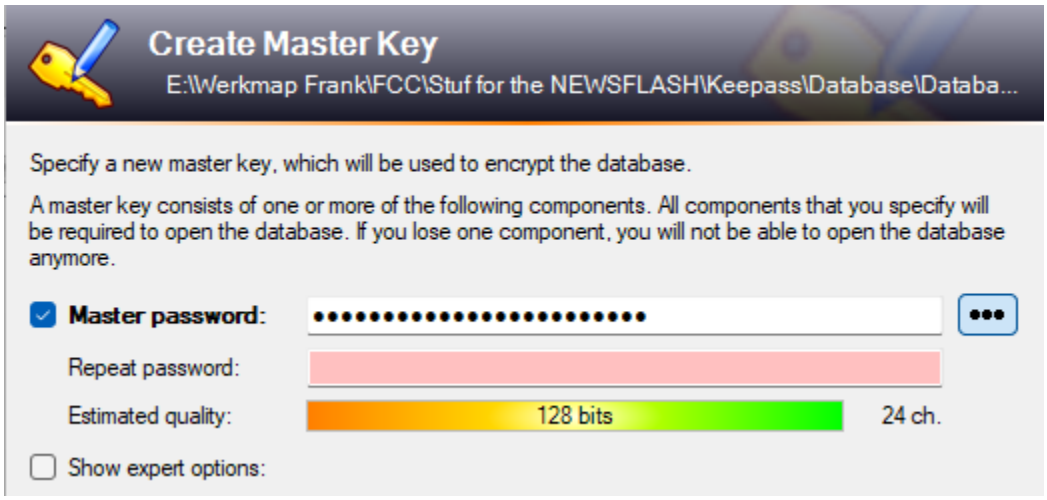
FREEWARE – 12/04/2026
PASWOORDEN BEHEREN MET KEEPASS

KeePass is een gratis en open-source wachtwoordmanager. Het programma is ontworpen om je wachtwoorden veilig op te slaan en te beheren.

Veiligheid is erg belangrijk voor dit programma. Hiervoor wordt er gebruikgemaakt van een sterke encryptie zoals AES-256 en ChaCha20 en wordt alles lokaal opgeslagen, daar waar de meeste wachtwoordmanagers hun gegevens gaan opslaan in de cloud.
KeePass slaat al je wachtwoorden op in één versleuteld databasebestand. Toegang krijgen tot het databestand gebeurt standaard via één hoofdwachtwoord. Dit is het enige wachtwoord dat je moet onthouden om toegang te krijgen tot al je opgeslagen accounts.
Installeren doe je via de officiële website van KeePass, waar je bij voorkeur de "Professional Edition" download. Je kan vrij kiezen tussen een portable versie of een te installeren versie. Beide werken hetzelfde.

Wanneer we het programma voor het eerst gebruiken, moeten we beginnen met het maken van een nieuwe database. Gebruik hiervoor het menu **File** en de optie **New**. Standaard krijgt dit bestand de naam *Database.kdbx* en wordt het opgeslagen in de map **Documenten**. Zowel de naam als de locatie kan je echter zelf aanpassen. Het is wel belangrijk dat je onthoudt waar het databasebestand is opgeslagen, want je kan best regelmatig een back-up van het databasebestand maken op een andere computer of een usb.
Wanneer je met meerdere computers werkt, kan je perfect de database kopiëren naar dat andere toestel.
We sluiten dit gedeelte af door te kiezen voor **Opslaan**.

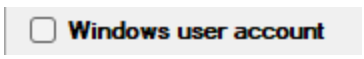
Zo komen we tot het belangrijkste onderdeel: het kiezen van een sterk en uniek wachtwoord.



Er zijn geen regels voor het paswoord (*zelfs 'OK' zou kunnen*), maar om echt veilig te zijn gebruik je best minimaal 12 tekens, waarvan hoofdletters, cijfers en symbolen.

Het venster heeft ook de optie: **Show expert options**. Je krijgt dan twee extra beveiligingsmogelijkheden: ***sleutelbestand/provider*** en ***Windows-gebruikersaccount***. Ik vermeld ze hier omdat ze aanwezig zijn, maar ik ben zeker niet geneigd om ze aan te raden. Er is het nodige gevaar aan verbonden.

- Een sleutelbestand kan worden gebruikt als onderdeel van de hoofdsleutel; het slaat geen databasegegevens op. Als een aanvaller toegang heeft tot het sleutelbestand, biedt dit geen bescherming. Let wel op: als het sleutelbestand verloren gaat of de inhoud ervan wordt gewijzigd, dan kan de database niet meer worden geopend. Je moet dus zeker zorgen dat je over een back-up van het sleutelbestand beschikt.

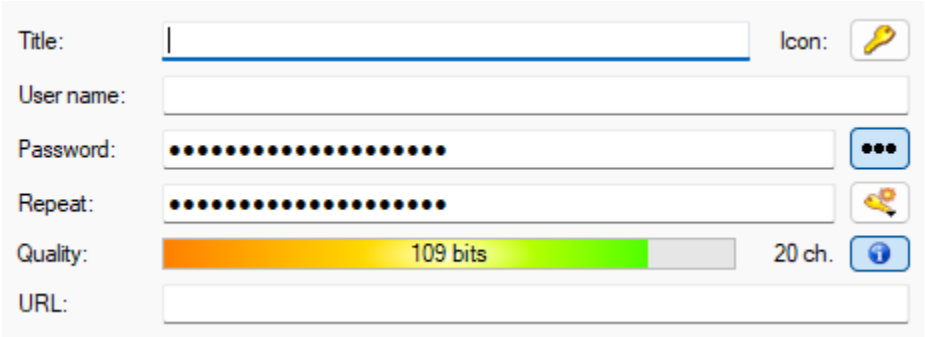


- Het Windows-gebruikersaccount gebruikt gegevens van het huidige Windows-gebruikersaccount. Deze gegevens veranderen niet wanneer het wachtwoord van het account wordt gewijzigd. Als het Windows-gebruikersaccount verloren gaat, is het niet voldoende om een nieuw account aan te maken met dezelfde gebruikersnaam en hetzelfde

wachtwoord. Een volledige back-up van het account is vereist. Het maken en herstellen van een dergelijke back-up is een zeer gecompliceerde taak.

Optioneel kan je ook nog een aantal extra instellingen voor de database toevoegen. Je kan je database een eigen naam geven, een beschrijving toevoegen of de encryptie-instellingen aanpassen. Dat laatste is zeker niet nodig, want de standaard is zeker goed genoeg.

Na al deze voorbereidingen kan je nu je lege kluis beginnen vullen. Klik hiervoor op het menu **Entry** en kies voor **Add Entry**.
Volgende gegevens kan je nu invullen: de titel of beschrijving van je paswoord, de gebruikersnaam, een wachtwoord (2x), een URL.
Het programma stelt zelf een sterk wachtwoord voor en geeft de sterkte ervan aan, maar je bent vrij om dit te aanvaarden of niet.
Via de mappen aan de linkerzijde kan je de wachtwoorden organiseren.



KeePass heeft heel wat voordelen: het is volledig gratis en open source, er is geen registratie nodig, het is zeer veilig en je bent niet afhankelijk van externe servers.

In onze programmabibliotheek vind je het programma samen met de nodige info.
U kan het programma ook zelf downloaden via onderstaande link.
https://keepass.info/download.html

FVG

Secretariaat
p/a
Moretuslei 3
B-2180 Ekeren

Informatie
Per post: via secretariaat
Per telefoon: 0032 3 2895573
Per e-mail: info@flanderscomputerclub.be

Lidgelden
60 EUR voor 1 jaar
IBAN: BE89 9734 5282 0585

Redactie: Frank Van Goolen